REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-01-2014	Final Report	25-Aug-2010 - 25-Oct-2013

4. TITLE AND SUBTITLE
High-Speed Large-Alphabet Quantum Key Distribution Using Photonic Integrated Circuits

5a. CONTRACT NUMBER
W911NF-10-1-0416

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

6. AUTHORS
Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Columbia University
615 West 131st Street
Room 254, MC 8725
New York, NY 10027 -7922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58496-PH-DRP.25

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
This program theoretically and experimentally investigated the private information capacity of optical channels under experimental constraints. Theoretical work established upper and lower bounds on the Holevo secrecy capacity for optical channels, including channels in turbulent atmosphere, and developed the coding and modulation techniques to approach the maximum key distribution rate over optical channels, in the regime of simultaneously high photon and bandwidth efficiencies. The program also developed two quantum key distribution (QKD) protocols that achieve an information capacity of multiple secure bits per photon pair, providing the first

15. SUBJECT TERMS
optical communications, quantum communication, quantum key distribution

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dirk Englund
UU	UU	UU	UU		19b. TELEPHONE NUMBER 617-324-7014

Report Title

High-Speed Large-Alphabet Quantum Key Distribution Using Photonic Integrated Circuits

ABSTRACT

This program theoretically and experimentally investigated the private information capacity of optical channels under experimental constraints. Theoretical work established upper and lower bounds on the Holevo secrecy capacity for optical channels, including channels in turbulent atmosphere, and developed the coding and modulation techniques to approach the maximum key distribution rate over optical channels, in the regime of simultaneously high photon and bandwidth efficiencies. The program also developed two quantum key distribution (QKD) protocols that achieve an information capacity of multiple secure bits per photon pair, providing the first security proofs for experimentally realizable high-dimensional QKD schemes against collective attacks. These protocols represent quantum secure versions of pulse-position- modulation schemes that are commonly employed in energy-constrained electromagnetic channels. Novel adaptive pulse-position modulation and layered coding schemes provide efficient error correction. The experimental effort developed QKD hardware in silicon photonic integrated circuits (PIC), including waveguide-integrated superconducting nanowire single photon detectors. Ultra-bright waveguide-based entangled pair generation was demonstrated with record high entanglement purity measured using dispersion-compensated Franson interferometry. QKD systems were demonstrated with secure key generation in excess of 6 Mbit/second and a photon efficiency in excess of 3 secure bits per detected photon.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 6.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
07/09/2013	19.00 Jeffrey H. Shapiro, Nivedita Chandrasekaran, Ligong Wang. Ultimate Limits on Photon and Spectral Efficient Communication through Atmospheric Turbulence, OSA Topical Meeting on Applications of Lasers for Sensing & Free Space Optical Communications. 01-OCT-13, . : ,

TOTAL: **1**

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper
07/04/2013	12.00 Yuval Kochman, Gregory W. Wornell. On High-Efficiency Optical Communication and Key Distribution, Information Theory and Applications (San Diego). 05-FEB-12, . : ,

TOTAL: **1**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper
01/20/2014 23.00	Catherine Lee, Jacob Mower, Zheshen Zhang, Jeffrey H. Shapiro, Dirk Englund. Finite-key analysis of high-dimensional time-energy entanglement-based quantum key distribution, ArXiv e-prints (11 2013)
01/20/2014 24.00	Zheshen Zhang, Jacob Mower, Dirk Englund, Franco N. C. Wong, Jeffrey H. Shapiro. Unconditional Security of Time-energy Entanglement Quantum Key Distribution using Dual-basis Interferometry, ArXiv e-prints (11 2013)
04/10/2012 11.00	Jeffrey H. Shapiro, Nivedita Chandrasekaran, Gregory W. Wornell, Ligong Wang. Private-Capacity Bounds for Bosonic Wiretap Channels, IEEE International Symposium on Information Theory (01 2012)
07/04/2013 16.00	Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, Dirk Englund. High-dimensional quantum key distribution using dispersive optics, Physical Review A (03 2013)
07/09/2013 17.00	Nivedita Chandrasekaran, Jeffrey H. Shapiro, Ligong Wang. Photon Information Efficient Communication Through Atmospheric Turbulence—Part II: Bounds on ErgodicClassical and Private Capacities, JOURNAL OF OPTICAL COMMUNICATION AND NETWORKING (07 2013)
07/09/2013 18.00	Nivedita Chandrasekaran, Jeffrey H. Shapiro. Photon Information Efficient Communication Through Atmospheric Turbulence—Part I: Channel Model and Propagation Statistics, J. OPT. COMMUN. NETW. (07 2013)
08/25/2011 6.00	Cheng-Chia Tsai, Jacob Mower, Dirk Englund. Directional free-space coupling fromphotonic crystal waveguides, Optics Express (08 2011)
08/25/2011 7.00	Jacob Mower, Dirk Englund. Efficient generation of single and entangled photons on a siliconphotonic integrated chip, (08 2011)
09/29/2013 21.00	X. Gan, R.J. Shiue, Y. Gao, I. Meric, T. F. Heinz, K. Shepard, J. Hone, S. Assefa, D. Englund. Chip-integrated ultrafast graphene photodetector with high responsivity, , Nature Photonics (03 2013)
09/29/2013 22.00	Tian Zhong, Franco N. C. Wong. Nonlocal cancellation of dispersion in Franson interferometry, PHYSICAL REVIEW A (12 2012)

TOTAL: 10

Number of Manuscripts:

Books

Received Paper

TOTAL:

Patents Submitted

CHIP INTEGRATED SINGLE PHOTON GENERATION BY ACTIVE TIME MULTIPLEXING
COMPACTLY INTEGRATED OPTICAL DETECTORS AND ASSOCIATED SYSTEMS AND METHODS
Cavity-Enhanced Atomic-Force Microscope on-Fiber
Chip-Scale Hyperentanglement Analysis, Generation, and SWAP Gates
GRAPHENE PHOTONICS FOR RESONATOR-ENHANCED ELECTRO-OPTIC DEVICES AND ALL-OPTICAL INTERACTIONS
SYSTEMS AND METHODS FOR COUPLING ELECTROMAGNETIC RADIATION FROM FIBER ARRAYS INTO WAVEGUIDES AND PHOTONIC CHIPS
SYSTEMS AND METHODS FOR TELECOMMUNICATION USING HIGH-DIMENSIONAL TEMPORAL QUANTUM KEY DISTRIBUTION

Patents Awarded

Awards

Englund: 2011 AFOSR PECASE; 2012 IEEE-HKN Outstanding Young Professional Award; 2012 IBM Faculty Award; 2011 Sloan Research Fellowship in Physics

Shapiro: Fellow of the SPIE; MIT Lincoln Laboratory Best Paper Award

Franco Wong: Fellow of the OSA

Chee Wei Wong: Fellow of the OSA

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Jacob Mower	0.60	
Pierre Desjardins	0.50	
Nivedita Chandrasekaran	0.00	
Andrew Dane	1.00	
Faraz Najafi	1.00	
Tian Zhong	1.00	
XinAn Xu	1.00	
FTE Equivalent:	**5.10**	
Total Number:	**7**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Xiaolong Hu	1.00
Ligong Wang	0.00
Zheshen Zhang	0.50
Hongchao Zhou	0.50
Zhenda Xie	0.50
FTE Equivalent:	**2.50**
Total Number:	**5**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Dirk Robert Englund	0.06	
Jeffrey H. Shapiro	0.03	No
Chee Wei Wong	0.03	
Karl Berggren	0.03	
Gregory Wornell	0.05	
FTE Equivalent:	**0.20**	
Total Number:	**5**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 5.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 5.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 5.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 5.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME
Pierre Desjardins
Jacob Mower
Total Number: **2**

Names of personnel receiving PHDs

NAME
Tian Zhong, 2013 (MIT)
Total Number: **1**

Names of other research staff

NAME	PERCENT_SUPPORTED
Franco N.C. Wong	0.10
FTE Equivalent:	**0.10**
Total Number:	**1**

Sub Contractors (DD882)

Inventions (DD882)

5 **Cavity-Enhanced Atomic-Force Microscope on-Fiber**

Patent Filed in US? (5d-1) N

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) N

Foreign Countries of application (5g-2):

5a: Dirk Englund

5f-1a:

5f-c:

5a: Xiaolong Hu

5f-1a:

5f-c:

5 **CHIP INTEGRATED SINGLE PHOTON GENERATION BY ACTIVE TIME MULTIPLEXING**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: Jacob Mower

5f-1a:

5f-c:

5a: Dirk Englund

5f-1a: Columbia University

5f-c:

5 **Chip-Scale Hyperentanglement Analysis, Generation, and SWAP Gates**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) N

Foreign Countries of application (5g-2):

5a: Dirk Englund

5f-1a:

5f-c:

5a: Franco N. C. Wong

5f-1a: MIT

5f-c:

5a: Chee Wei Wong

5f-1a: Columbia University

5f-c:

5 **COMPACTLY-INTEGRATED OPTICAL DETECTORS AND ASSOCIATED SYSTEMS AND METHODS**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2): international patent application

5a: Jacob Mower

5f-1a:

5f-c:

5a: Dirk Englund

5f-1a:

5f-c:

5a: Xiaolong Hu

5f-1a:

5f-c:

5a: Karl Berggren

5f-1a:

5f-c:

5a: Faraz Najafi

5f-1a:

5f-c:

5 **GRAPHENE PHOTONICS FOR RESONATOR-ENHANCED ELECTRO-OPTIC DEVICES AND ALL-OPTICAL IN- T**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: Xuetao Gan

5f-1a: Columbia University

5f-c:

5a: Dirk Englund

5f-1a: Columbia University

5f-c:

5 **SYSTEMS AND METHODS FOR COUPLING ELECTROMAGNETIC RADIATION FROM FIBER ARRAYS INTO W**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) N

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2):

5a: Jacob Mower

5f-1a: Columbia University

5f-c:

5a: Dirk Englund

5f-1a: Columbia University

5f-c:

5 **SYSTEMS AND METHODS FOR TELECOMMUNICATION USING HIGH-DIMENSIONAL TEMPORAL QUAN- TU**

Patent Filed in US? (5d-1) Y

Patent Filed in Foreign Countries? (5d-2) Y

Was the assignment forwarded to the contracting officer? (5e) Y

Foreign Countries of application (5g-2): international patent application

5a: Dirk Englund

5f-1a: Columbia University

5f-c:

5a: Jacob Mower

5f-1a: Columbia University

5f-c:

5a: Jacob Mower

5f-1a: Columbia University

5f-c:

5a: Pierre Desjardin

5f-1a: Columbia University

5f-c:

Scientific Progress

Technology Transfer

High-Speed Large-Alphabet Quantum Key Distribution Using Photonic Integrated Circuits

Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong,
Franco Wong, and Gregory Wornell

Abstract

This program theoretically and experimentally investigated the private information capacity of optical channels under experimental constraints. Theoretical work established upper and lower bounds on the Holevo secrecy capacity for optical channels, including channels in turbulent atmosphere, and developed the coding and modulation techniques to approach the maximum key distribution rate over optical channels, in the regime of simultaneously high photon and bandwidth efficiencies. The program also developed two quantum key distribution (QKD) protocols that achieve an information capacity of multiple secure bits per photon pair, providing the first security proofs for experimentally realizable high-dimensional QKD schemes against collective attacks. These protocols represent quantum secure versions of pulse-position- modulation schemes that are commonly employed in energy-constrained electromagnetic channels. Novel adaptive pulse-position modulation and layered coding schemes provide efficient error correction. The experimental effort developed QKD hardware in silicon photonic integrated circuits (PIC), including waveguide-integrated superconducting nanowire single photon detectors. Ultra-bright waveguide-based entangled pair generation was demonstrated with record high entanglement purity measured using dispersion-compensated Franson interferometry. QKD systems were demonstrated with secure key generation in excess of 6 Mbit/second and a photon efficiency in excess of 3 secure bits per detected photon.

Contents

1 Introduction

To understand the limits of optical communications, it is necessary to consider light at the level of photons, described by quantum theory. This theory has profound consequences, including the possibility of transmitting information in unconditionally secure ways [1]. This report addresses open questions, including the information capacity and transfer rate of optical channels, which are not only of fundamental importance in information science, but are also of increasing technological relevance in emerging communication systems that offer new possibilities in terms of speed, security, and power consumption. We summarize the results of experimental and theoretical investigations on the fundamental information capacity of optical communications and the development of new quantum cryptographic protocols that approach these capacities, and we summarize experimental advances at the device and system level that have enabled quantum key distribution, secure against collective attacks, at greater than one bit per detected photon pair and faster than 3 Mbit/s.

The report is organized as follows. Section 2 addresses fundamental limits of privacy capacities of optical communications. Upper and lower bounds for the ergodic Holevo capacities of private information transmission are derived over the multiple spatial-modes in a turbulent channel. Section 3 describes new types of large-alphabet QKD protocols employing high-dimensional correlations in temporal and spectral degrees of freedom of entangled photon pairs. We demonstrate security proofs based on entanglement visibility estimates based on Alice's and Bob's measurements in two conjugate bases. In one protocol, the basis transformations are realized using dispersive optical elements [2]. In the other protocol, the visibility is estimated based on measurements in Franson interferometers [3]. Section 4 describes the hardware developed for implementing high-dimensional QKD schemes, focusing on (i) the photonic integrated circuit (PIC) architecture, (ii) an ultrabright source of entangled degenerate telecom-band photon pairs based on a PPKTP waveguide, (iii) high-visibility Franson interferometry, and (iv) PIC integration of superconducting nanowire single photon detectors (SNSPDs). Section 5 discusses the QKD system demonstrations, including novel coding schemes for high-efficiency error correction specifically tailored to high-alphabet QKD schemes.

2 Information Capacity of a Photon and Transmission in Free Space

Of fundamental importance in reaching high photon efficiency (many bits/detected photon) is to understand the potential benefit of using multiple spatial modes. The benefit is not obvious: while the use of multiple spatial modes increases the alphabet size of entangled photon pairs (through hyperentanglement), it comes at the cost of increased errors due to cross-talk and potentially increased channel loss. To understand these trade-offs, MIT analyzed the information capacity of optical communications in free space using multiple spatial modes under an average photon-number constraint [4, 5]. The problem statement is illustrated in Fig. 1.

Optical communication with high photon efficiency (many bits/photon) and high spectral efficiency (bits/sec-Hz) is possible only through the use of multiple spatial modes. For

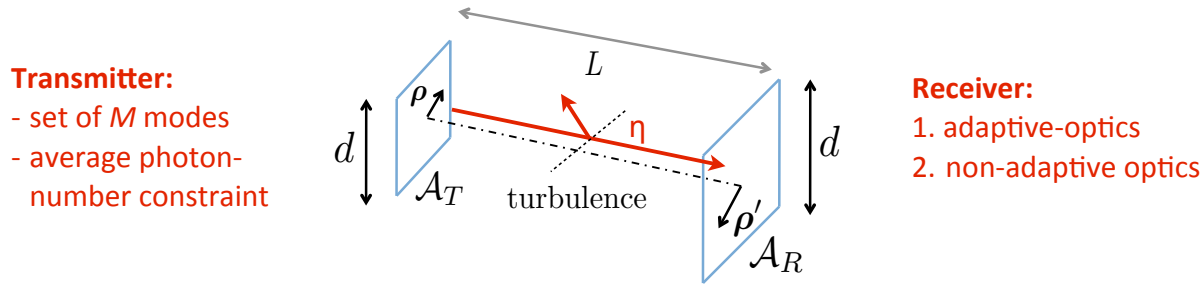

Figure 1: Optical communication over M spatial modes under average photon-number constraint. The notional beam splitter represents the random sub-unity transmissivity, η, of an arbitrary transmitted spatial mode.

instance, at the Holevo limit, 189 spatial modes would enable 10 bits/photon and 5 bits/sec-Hz, but a joint-detection receiver, for which no explicit realization has been demonstrated, would be needed to achieve this performance. On the other hand, it should be possible to approach the Shannon limit for binary encoding and direct detection with available equipment, but 4500 spatial modes would be necessary for such a system to achieve 10 bits/photon and 5 bits/sec-Hz. Moreover, all of these performance figures assume equal-transmissivity spatial modes that retain their orthogonality after propagation through the channel. In practical scenarios employing atmospheric or optical fiber links, mode-dependent loss and intermodal cross-talk must be taken into account. MIT derived power transmissivity bounds and intermodal cross-talks for the turbulent channel. These bounds depend only on the mutual coherence function of the atmospheric Green's function, and thus apply in both weak and strong turbulence and can be evaluated for arbitrary turbulence distributions along the propagation path.

The MIT team showed that any multiple-mode noiseless bosonic wiretap channel is equivalent to a group of parallel (i.e., noninterfering) single-mode channels. Then, the total channel capacity can be computed from the optimal allocation of photons to the M modes. Fig. 2 shows the ergodic holevo secrecy capacities for sets of ∼200 focused-beam (FB), Hermite-Gaussian (HG), and Laguerre-Gaussian (LG) modes. These were evaluated for operation with adaptive and non-adaptive receivers for realistic values of uniformly-distributed turbulence, as detailed in Ref. [5]. These plots point to the following major results:

- bounds on ergodic Holevo secrecy capacities for near-field operation with adaptive-optics and non-adaptive receivers
- bounds evaluated for FB, HG, and LG modes
- HG and LG modes shown to have same ergodic Holevo secrecy capacities
- FB modes outperform HG and LG modes when adaptive optics are employed
- HG and LG modes outperform FB modes when adaptive optics are not employed

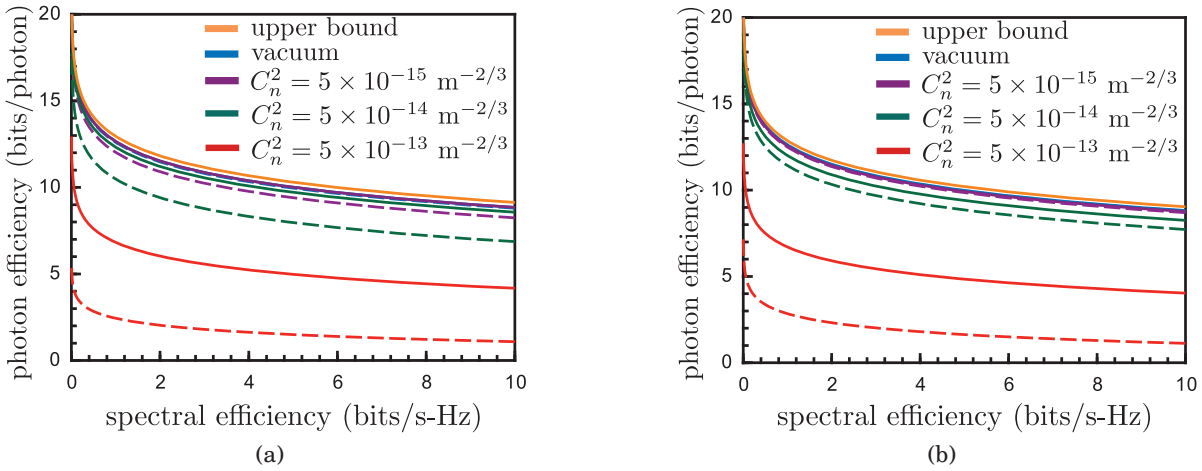

Figure 2: Upper and lower bounds on photon information efficiency, as functions of spectral efficiency, of the ergodic Holevo private capacities for: (a) $M = 225$ FB-mode systems; and (b) $M = 231$ HG or LG systems. These results assume square-pupil transmitters and receivers with identical d = 17.6 cm side lengths, and operation at $\lambda = 1.55\,\mu$m wavelength over an $L = 1$ km propagation path. Solid lines are for systems with perfect adaptive optics, while dashed lines are for systems without adaptive optics.

2.1 Secrecy of Bosonic Wiretap Channel

The Wornell group has investigated the secrecy capacity of the bosonic wiretap channel. The team has proved a new upper bound on the secrecy capacity of the bosonic wiretap channel. This bound does not rely on any unproven conjecture, including the entropy photon-number inequality [6].

3 QKD Protocols

High-dimensional quantum key distribution (QKD) [7] allows two parties, Alice and Bob, to establish a secure cryptographic key at a potentially higher rate than that afforded by standard, two-dimensional QKD protocols [8, 9]. When the photonic states are measured using a high-dimensional Hilbert space, more than one bit of information can be generated when a single photon is detected. Additionally, increasing the dimension of a QKD protocol provides greater resilience to noise [10]. High-dimensional QKD protocols have been implemented by encoding information in various photonic degrees of freedom, including position-momentum [11], time [12, 13, 14, 15], energy-time [16], and orbital angular momentum (OAM) [17, 18, 19]. Because we desired a protocol that is maximally compatible with modern-day fiber communications systems, we focused on the use of temporal encoding of information.

The time-energy entanglement of photon pairs produced by spontaneous parametric downconversion was previously used in high-dimensional experiments [12, 20], but these works lacked rigorous security proofs. Security proofs for time-energy entanglement-based HDQKD have been attempted by discretizing the continuous Hilbert space to permit use

of discrete-variable security analyses [21, 22], but the validity of the discretization approach has not been proven and it only provides security against individual attacks. We developed security proofs that combine the best elements of discrete-variable and continuous-variable security analysis [23, 24]. In particular, the latter employs the quadrature-component covariance matrix to derive a lower bound on the secure-key rate in the presence of a collective attack. In the two high-dimensional QKD schemes developed in this program, we took an analogous approach by bounding Eve's information from an estimate of the time-frequency covariance matrix. The two protocols differ in the experimental implementation in which the relevant covariance matrices are estimated. In 'Dispersive Optics' QKD (DO-QKD) [25], the covariance matrix is estimated from Alice's and Bob's measurements performed with our without group velocity dispersion. In the other protocol, we employ dual-basis interferometry to estimate the covariance matrix from correlation measurements performed in Franson and conjugate-Franson interferometers [3].

3.1 Dispersive Optics Quantum Key Distribution

Using a high-dimensional alphabet, the DO-QKD protocol is closely analogous to pulse position modulation (PPM) to maximize the secret-key capacity under technical constraints such as limited numbers of photon produced or limited number of detector clicks per unit time. We have completed a thorough analysis of the DO-QKD protocol, proving security against collective attacks.

Alice and Bob build a secure key by measuring the arrival times of entangled photons. To start, Alice shares a clock with Bob and generates a biphoton state by spontaneous parametric down conversion (SPDC). In the weak pumping regime, the down-converted state can be approximated by $|\Psi_{AB}\rangle = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \psi(t_A, t_B)\,|t_A, t_B\rangle\, dt_A dt_B$, where $|t_A, t_B\rangle = \hat{a}_A^\dagger(t_A)\hat{a}_B^\dagger(t_B)\,|0\rangle$ and $\hat{a}_A^\dagger(t_j)$ ($\hat{a}_B^\dagger(t_j)$) denotes the creation operator at time t_j for Alice (Bob). We approximate $\psi(t_A, t_B) \propto \exp[-(t_A - t_B)^2/4\sigma_{cor}^2]\exp[-(t_A + t_B)^2/16\sigma_{coh}^2]\exp[i\omega_p/2\cdot(t_A + t_B)]$, where σ_{coh} is the coherence time of the pump field at ω_p and the correlation time, σ_{cor}, is given by the phase matching bandwidth of the SPDC crystal. $|\Psi_{AB}\rangle$ therefore describes the superposition of photon pair states with duration of order σ_{cor} over a period of order σ_{coh}.

In the protocol, Alice and Bob measure their photon's time of arrival randomly either directly or in a conjugate basis. They build the key from the correlated timing events from in the same (publicly compared) basis choices, using error correction and privacy amplification [26].

A crucial question concerns the implementation of the conjugate basis measurement. We shoed that conjugate basis measurements are achieved using a unitary transformation $\hat{U}$ that can be easily implemented using second-order dispersion (SOD), characterized by the parameter $\beta_2 = \partial^2/\partial\omega^2(n_{\text{eff}}\omega/c)$, where n_{eff} is the effective index of the mode, ω is the mode frequency, and c is the speed of light in vacuum. A second-order dispersive element imparts a phase on each frequency state $\phi \propto \beta_2\omega^2$. Physically, β_2 is proportional to the linear change in the group velocity as a function of frequency. The SOD operator is unitary and its frequency domain representation, $\hat{\Delta}$ is diagonal.

Classically, a transform-limited pulse is spread in a dispersive medium as its frequency

components move out of phase. However, Ref. [27] showed that if the entangled photons pass through dispersive media, in the limit of large $\sigma_{\rm coh}$, $\sigma_{\rm cor}$ becomes

$$\sigma'^2_{\rm cor} \approx \frac{\sigma^4_{\rm cor} + (\beta_{2A}L_A + \beta_{2B}L_B)^2}{\sigma^2_{\rm cor}}, \tag{1}$$

where β_{2A} (β_{2B}) is the GVD introduced by Alice (Bob) over length L_A (L_B). Assume that $L_A = L_B = L$ and $\beta_{\rm tot} = \beta_{2A} + \beta_{2B}$. As $\beta_{\rm tot}$ increases, the temporal correlation between Alice's and Bob's photon decreases. However, $\sigma'_{\rm cor} = \sigma_{\rm cor}$ if $\beta_{2A} = -\beta_{2B} = \beta_2$, which requires that, to a global phase, $\hat{\Delta}_A = \int e^{-i\frac{1}{2}\beta_{2A}L\omega_o^2} |\omega_o\rangle \langle\omega_o| \, d\omega_o = \hat{\Delta}_B^\dagger$, where ω_o is the frequency detuning from the center frequency of the biphoton pulse. Thus, if Alice applies normal dispersion, $\hat{U}_A$, on her photon, Bob can apply anomalous dispersion, $\hat{U}_B = \hat{U}_A^\dagger$, on his photon to recover the temporal correlations between their photons. Thus, Alice and Bob's measurements in the 'dispersed' basis are also correlated, as required.

In Ref. [25], we proved security against general coherent attacks through measurements by Alice and Bob in two conjugate bases, which are implemented using only single-photon detectors and simple dispersive optics with group velocity dispersion (GVD). DO-QKD benefits from the robustness of temporal correlations in single-mode fiber and free space. We estimate that practical implementations could reach a secret-key capacity of ~ 3 bits/photon over up to ~ 250 km of fiber. Fig. 3 shows the secret-key capacity calculated from covariance matrix approach to establish an upper bound on Eve's information given collective attacks.

3.2 Quantum Key Distribution using Dual-basis Interferometry

As was shown, the dispersive-optics scheme enables measurements of the time-frequency covariance matrix. However, commercial dispersive optics elements with high group velocity dispersion can can introduce significant loss of approximately 3 dB for each party. A potentially simpler technique experimentally—utilizing a Franson interferometer (FI)—was conjectured [12, 20] to suffice for security verification. Its robustness against some specific attacks has been discussed [20, 28], but security against collective attacks had not been proven, and [28] suggests such a proof may be impossible.

We recently showed that time-energy entanglement-based HDQKD can be made secure against Eve's collective attack when a Franson interferometer is used for security verification, together a frequency-difference measurement based on dispersion. The proof relates the fringe visibility of the Franson interferometer to the time-frequency covariance matrix. Together with the frequency-difference measurement, these measurements upper-bound Eve's Holevo infor-

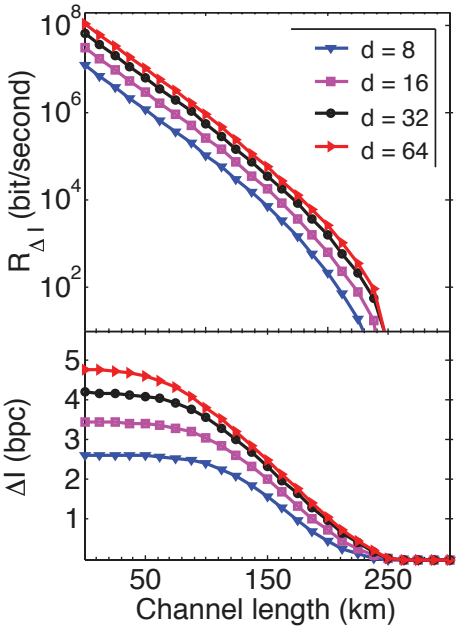

Figure 3: Top: key generation rate (bits/second). Bottom: Secret key capacity ΔI in units of bits per clicks (bpc), postselected for frames in which both Alice and Bob register at least one detector click.

mation, enabling a calculation of Alice and Bob's secure key capacity.

Details of the protocol are reported in Ref. [3]; we replicate here the key generation rate and photon efficiency in terms of bits per coincidence. As in the DO-QKD protocol, we assume superconducting detectors with realistic (demonstrated) performance figures and high Franson visibility already demonstrated by members of this team [29]. Figure 4's left panel plots Alice and Bob's SKR versus transmission distance for two frame durations and two system efficiencies for Alice (η_A) and Bob's (η_B) receivers. We see that low-efficiency SNSPDs allow QKD out to 200 km, while high-efficiency SNSPDs promise QKD out to 300 km, and going from 15% to 90% system efficiency increases the SKR by approximately two orders of magnitude.

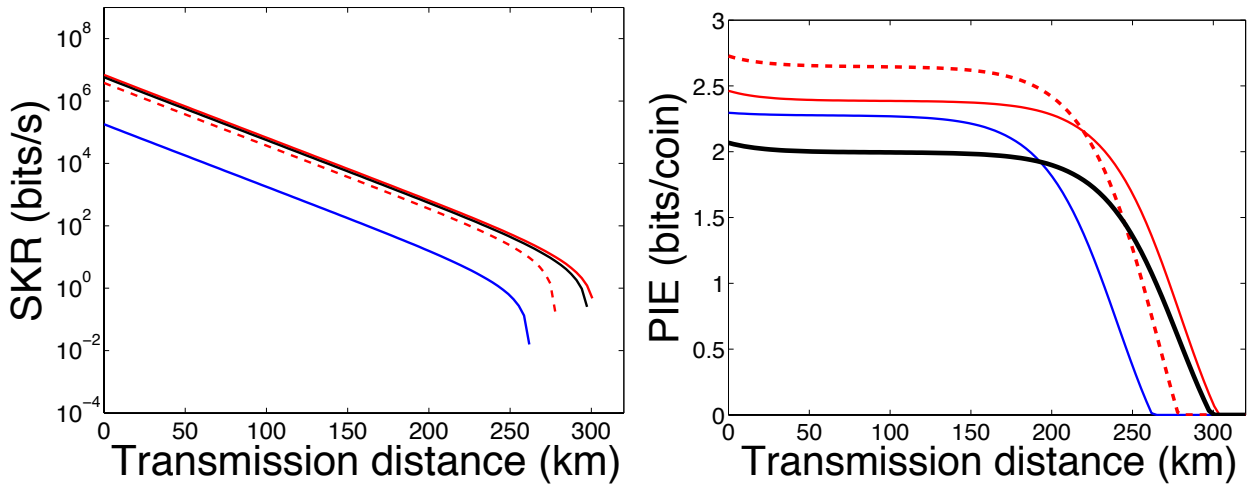

Figure 4: Left panel: Alice and Bob's SKR versus transmission distance. Right panel: Alice and Bob's PIE versus transmission distance. Details on assumed experimental parameters are provided in Ref. [3].

4 Hardware

4.1 Photonic Integrated Chip

Photonic integrated circuits (PIC) offer a robust and scalable platform for fundamental quantum optics experiments and quantum communication technologies. We have developed a PIC architecture to implement the two QKD protocols described above.

Dual-Basis Interferometry (Sect. 3.2): Alice and Bob have identical chips which contain a photonic integrated circuit (PIC) for the key generation and the security check. An incident photon on Alice's or Bob's setup is analyzed either (1) directly on a photon detector or (2) after a Mach Zehnder interferometers that makes up one half of a Franson interferometer, which enables a measurement of the degree of entanglement between the two photons [30]. These measurements corresponds to projections in two bases, (1) and (2). A measurement by Eve reduces the entanglement, which could be detected in the Franson fringe visibility [3].

The optical circuit that implements these measurements is illustrated in Figure 5, in which the 'X' symbols represent switches that randomly channel photons between 'key generation' and 'security check' (the two switches in Bob's or Alice's setup are synchronized.)

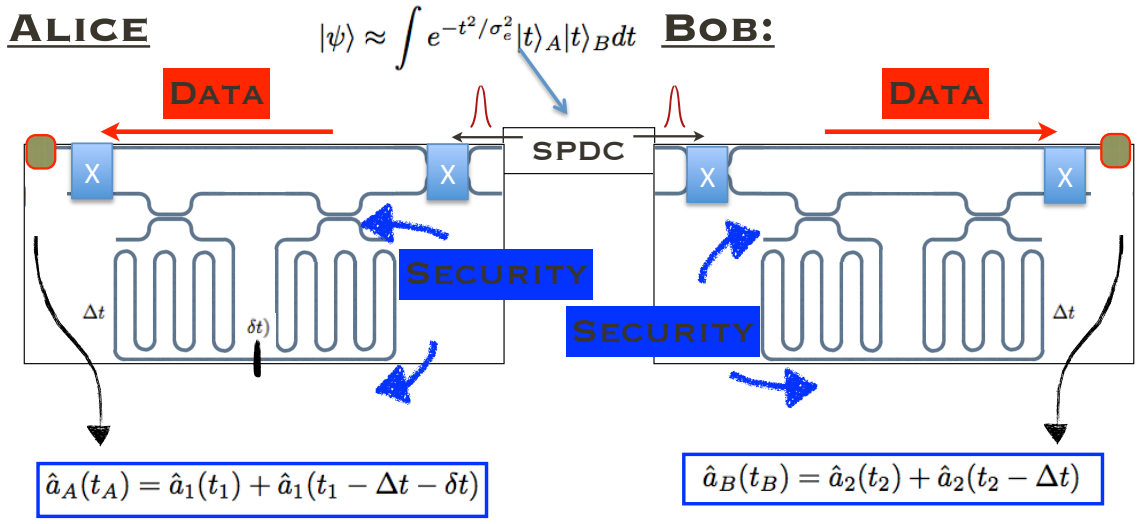

Figure 5: An entangled photon state is generated by spontaneous parametric down conversion; this is approximated at the biphoton given in the top of the figure. One photon is sent to Alice, the other to Bob. These parties either measure the timing of the photon pair to establish a private key, or they check the security of the protocol using a Franson interferometer. The Franson interferometer employs two unbalanced MZ interferometers with time-difference Δt, enabling coherence measurements to $2\Delta t$. A small path difference δt is used to change the coincidence probability from maximum to minimum.

PICs were designed and fabricated in collaboration with Dr. Solomon Assefa at the IBM T.J. Watson Research Center IBM in Yorktown Heights, New York. They were fabricated using 193-nm optical lithography, followed by dry etching to define channel waveguides. Coupling to and from the chip was done through tapered Si waveguides coupled to polymer and silicon nitride (SiN) edge couplers. Fig. 6 shows on-chip Franson interferometers, consisting of two unbalanced MZIs with a 300 ps path-length difference in the form of a meander waveguide. Photons coupled into the PIC are either directed directly to a single photon detector for key generation, or they can be directed into the MZI to perform the security check, as discussed in Sect. 3.2 and Ref. [3].

How this routing is performed can be seen from the close-up image of the waveguide/MZI interface in Fig. 7. The three-ring structures provides a $\sim$ 2 nm bandpass drop filter into the MZI. The multi-ring structure enables the creation of a top-hat transmission function, as opposed to the Lorentzian function for a single ring [31]. The splitting ratio is tunable by shifting the drop filter resonance with respect to the (fixed) biphoton frequency band, using optical carrier injection into the rings. Typically, both three-ring drop filters would be switched simultaneously. The switching was confirmed at speeds in excess of 1 GHz, using 800 nm tuning pulses provided by a Ti:Sapphire mode-locked laser.

Figure 8 shows experimental measurements of the on-chip Franson interferometers. In

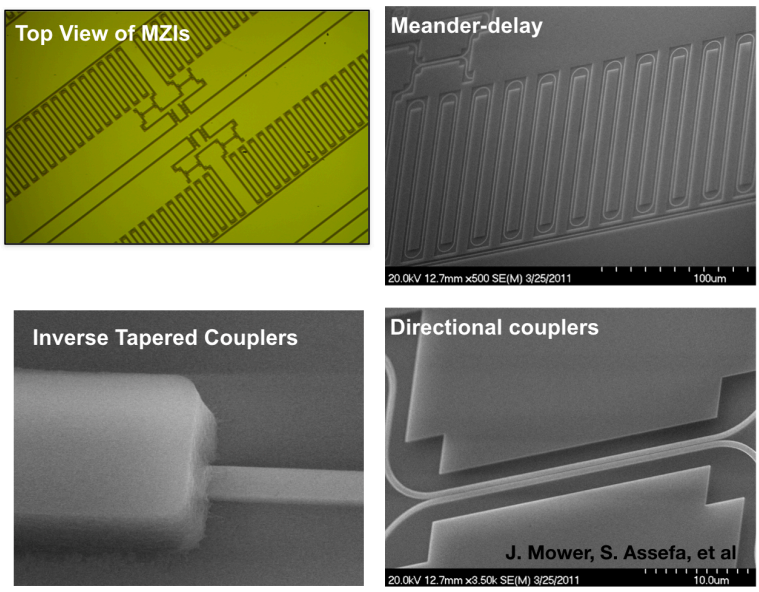

Figure 6: Counterclockwise from top left: (i) An optical micrograph of the PIC, showing two unbalanced MZIs with tunable drop filters for selecting key generation or security check. (ii) Close-up SEM of directional coupler. (iii) Close-up of inverse tapered waveguide edge couplers, at the location of the polymer waveguide/silicon channel waveguide interface. (iv) SEM of MZI/filter region, showing here a 5-ring drop filter configuration as in Ref. [31].

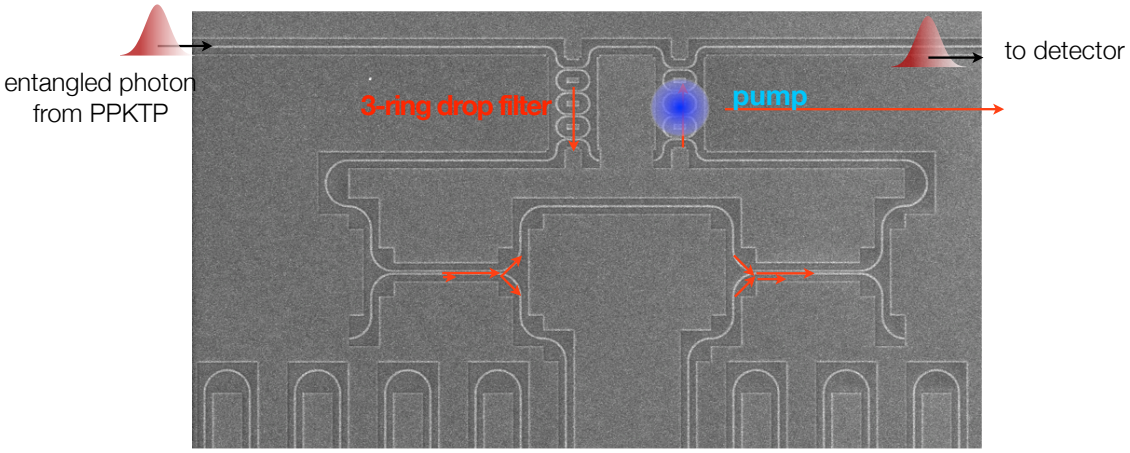

Figure 7: Close-up of a MZI/drop filter network, shown here in the 3-ring drop filter configuration.

this experiment, entangled photon pairs were generated using SPDC in a PPKTP waveguide. These photons, which were degenerate at 1550 with a 2-nm bandwidth, were coupled into two on-chip PICs located 5 meters apart. One of the PICs was temperature-tuned with respect to the other to realize a path length tuning between their two arms, as illustrated in Fig. 8(a). The classical and 4th order interference results are shown in Fig. 8(b) and (c), respectively. In these experiments, the directional couplers had to be tuned to compensate for the large waveguide loss in the longer MZI arm. This required approximately a splitting

ratio of approximately 72/28. This imbalance was not perfectly achieved, causing a loss in interference visibility. Other devices are currently being investigated to improve the interference visibility above the 70% observed thus far. We note that these are the first chip-based Franson interferometer measurements reported to date. In addition to on-chip Franson interferometers, these PICs were used for on-chip integration of graphene detectors [32] and SNSPDs [33].

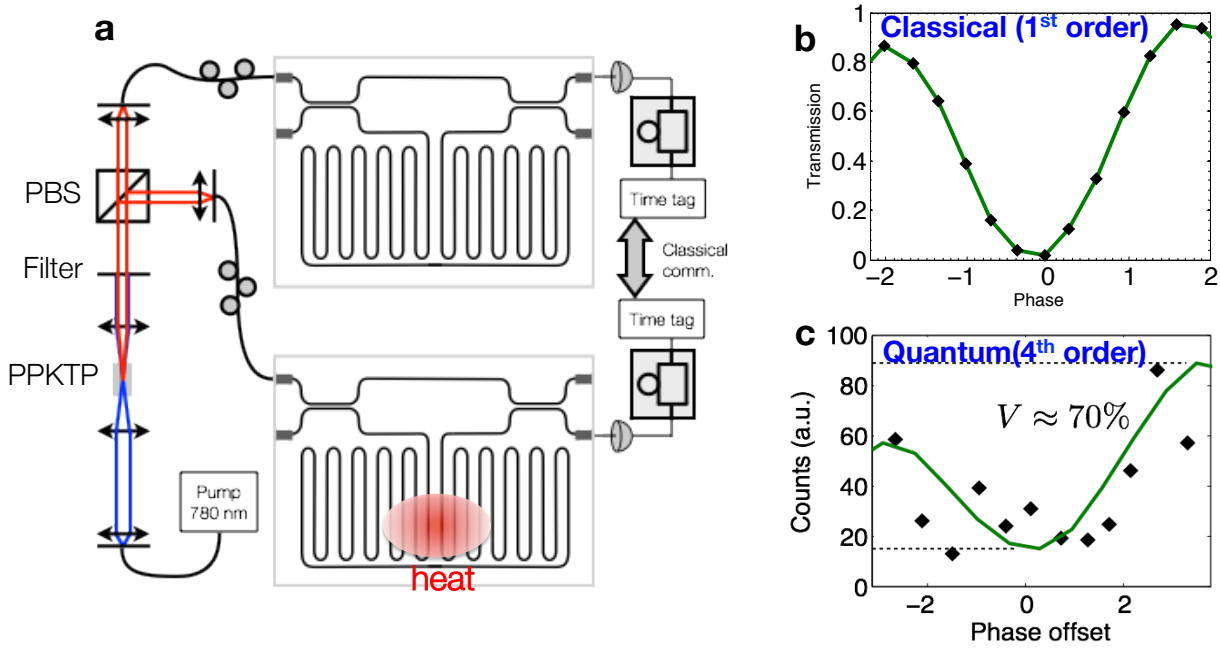

Figure 8: (a) Experimental setup: Degenerate telecom-wavelength photon pairs are generated using a PPKTP waveguide source, then signal and idler are separated by polarization and coupled into two separate PICs about 5 meters apart. The visibility is measured from coincidences on the outputs of the two unbalanced MZIs. The phase is thermally modulated on one of the MZIs. (b) First-order coherence function measured for one of the MZIs. [[[MUST STILL connect this to Franson visibility]]] (c) Coincidences measured across both MZIs indicates a visibility of 70%.

The Wong group demonstrated the highest Hong-Ou-Mandel visibility on-chip till date [34]. This is performed in the near-infrared with nanofabricated silicon nanophotonic directional couplers, with raw visibilities on-chip up to 90.5%. Spectrally-bright 1557-nm two-photon states are generated in a periodically-poled KTiOPO4 waveguide chip, serving as the entangled photon source and pumped with a self-injection locked laser, for the photon statistical measurements, as shown in Fig. **??**. Efficient four-port coupling in the communications C-band and in the high-index-contrast silicon photonics platform is demonstrated, with matching theoretical predictions of the quantum interference visibility as summarized in Fig. 10. Constituents for the residual quantum visibility imperfection are examined, supported with theoretical analysis of the sequentially-triggered multipair biphoton (Fig. 11), towards scalable high-bitrate quantum information processing and communications. The on-chip HOM interference is useful towards scalable high-bitrate quantum information processing and communications.

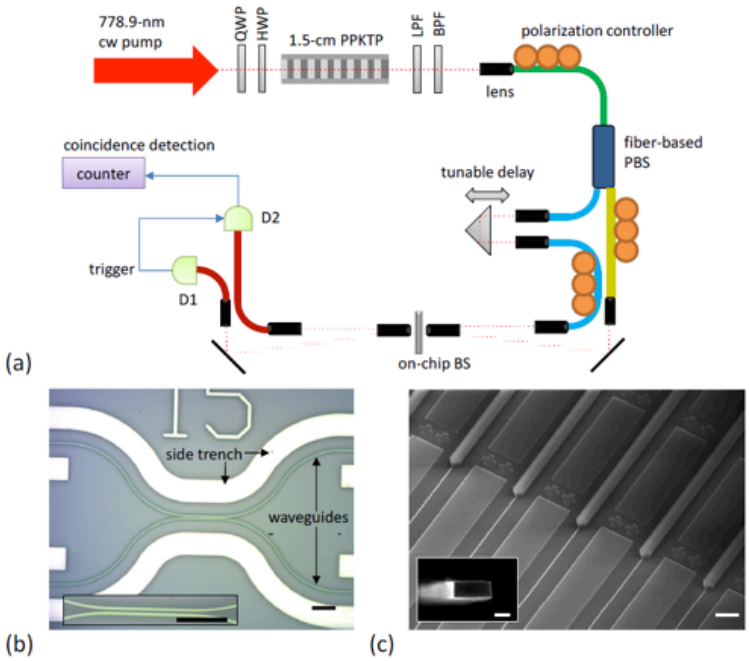

Figure 9: (a) Experiment setup for near-infrared Hong-Ou-Mandel interference in silicon quantum photonic chip. Fiber polarization controllers are used to ensure biphoton splitting via fiber polarization beam splitter, and to equalize the TM polarization coupling onto the silicon chip. The photon statistics are collected with one single photon detector triggering the other to diminish the dark counts and accidentals. QWP: quarter-wave plate; HWP: half-wave plate; LPF: low-pass filter; BPF: band-pass filter; PBS: polarization beam splitter; BS: beam splitter. (b) Optical micrograph of nanofabricated directional coupler in silicon-on-insulator. The side trenches (in white) are intended to mark and locate the device. Inset: zoom-in optical micrograph of the waveguide directional. Both scale bars: 1-um. (c) SEM of silicon inverse taper couplers with top oxide cladding waveguides. Scale bar: 20-um. Inset: end-view of protruded silicon waveguide. Scale bar: 200-nm.

In addition, under this InPho program, the Wong group developed low-loss photonic chips with total fiber-waveguide-qubit Gate-waveguide-fiber insertion loss down to 3-dB or less, as one of the program milestones. This includes the fiber-waveguide coupling and scattering losses in the optical components on-chip. This also includes 1-ns delay lines on-chip, with total loss of a few dB. Other optical components developed under this program includes zero-phase-advance delay lines [35], polarization beam splitters, chip-scale interferometers, multiplexing elements, and arrayed input-output elements.

4.2 Ultrahigh Flux Entangled Photon Source

The SPDC sources is implemented using PPKTP crystal samples with 46.2 μm grating periods, one from Raicol and one from AdvR, to determine their phase matching curves. We have conducted tests that indicate that nonlinear coefficients and bandwidths are as expected, with Raicol crystal slightly more efficient than AdvR crystal. The phase matching wavelengths for degenerate operation are shifted to the blue of 1560 nm. MIT achieved a

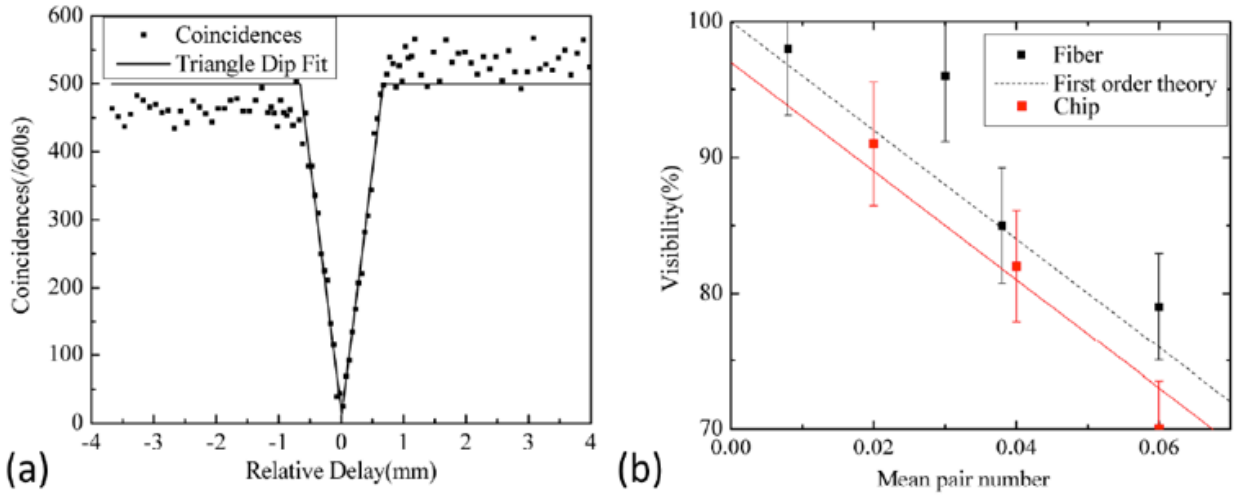

Figure 10: (a) Coincidences measured on the optimal directional coupler chosen experimentally with a splitting ratio (SR) less than 1-dB. A triangle fit is used for visibility estimation. A raw visibility of 90.5% is observed without accidental subtraction, and 90.8% with accidentals subtraction. (b) Visibility measured with different pump powers for both chip and fiber beam splitter implementations, for comparison. The visibility is approximately linearly related to the pump power as more probability of multiple biphoton pairs generated in one gate window. The first order theory is plotted as dashed line. The on-chip visibility is slightly lower than off-chip one by about 3%, which could be considered to be induced by the chip.

maximum pair generation rate of $8.9{\cdot}10^8$ pairs/s from a PPKTP waveguide at 89 mW pump power, as shown in Fig. 15.

4.3 Fiber-optic Franson interferometry

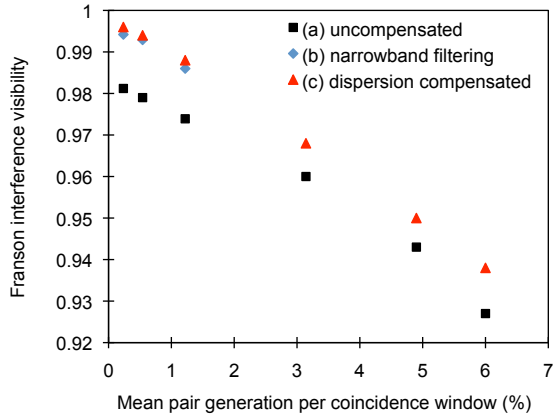

Figure 16: PPKTP photon pair generation.

Until recently, the maximum Franson visibility observed was limited to 98.2% [36]. This is surprising, since polarization measurements in the CHSH form of Bell's inequality violation show two-photon quantum-interference visibility of ¿99% [37, 38]. Why should entangled temporal degrees of freedom show lower visibility than polarization degrees of freedom? It was found by the MIT team that this limitation is due to dispersion between the long and short paths of the fiber loop in each arm [29]. Three cases were compared: (i) standard fiber loop, (ii) narrow bandpass filter for SPDC source to reduce the dispersion effect, and (iii) dispersion engineering with LEAF fiber to equalize the dispersion between the long and short paths (without the narrowband

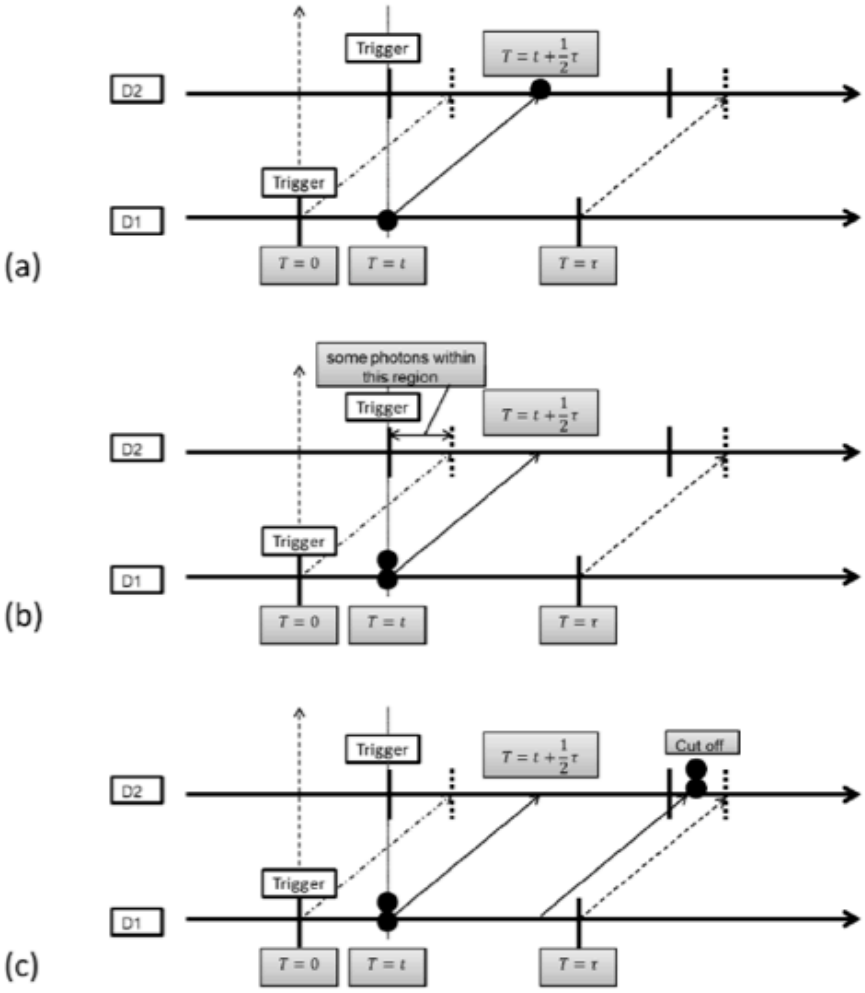

Figure 11: Scenario of the timeline for the photon pairs. (a) The delay of two photon pairs is set to $\tau/2$ to maximize the coincidences. (b) When there is only one photon pair in the gate window of D1, there is still possibility that D2 will record a photon event due to gate window time mismatch. (c) When there are two photon pairs within the gate window and separated to two detectors, there is possibility that the latter photon pair will be cut off due to the gate window time mismatch.

filter). Visibilities were observed of 98.2%, 99.4%, and 99.6% for the uncompensated case (i), the bandpass filtered case (ii), and the compensated unfiltered case (iii), respectively, as shown in Fig. 16. All were measured without background subtraction. The results clearly indicate that dispersion was the main cause of visibility degradation in uncompensated Franson interferometric measurements, and that we are now able to recover the lost visibility with dispersion engineering of the fiber loop. Details are reported in Ref. [29]. The high visibility we have obtained indicates the feasibility of dual-basis interferometry QKD described in Sect. 3.2.

In addition, under this program, the Wong group achieved the d-dimensional frequency-bin entanglement of a phase coherent mode-locked two-photon state in the infrared communications wavelengths. The high-dimensional mode-locked state exhibits the long-postulated

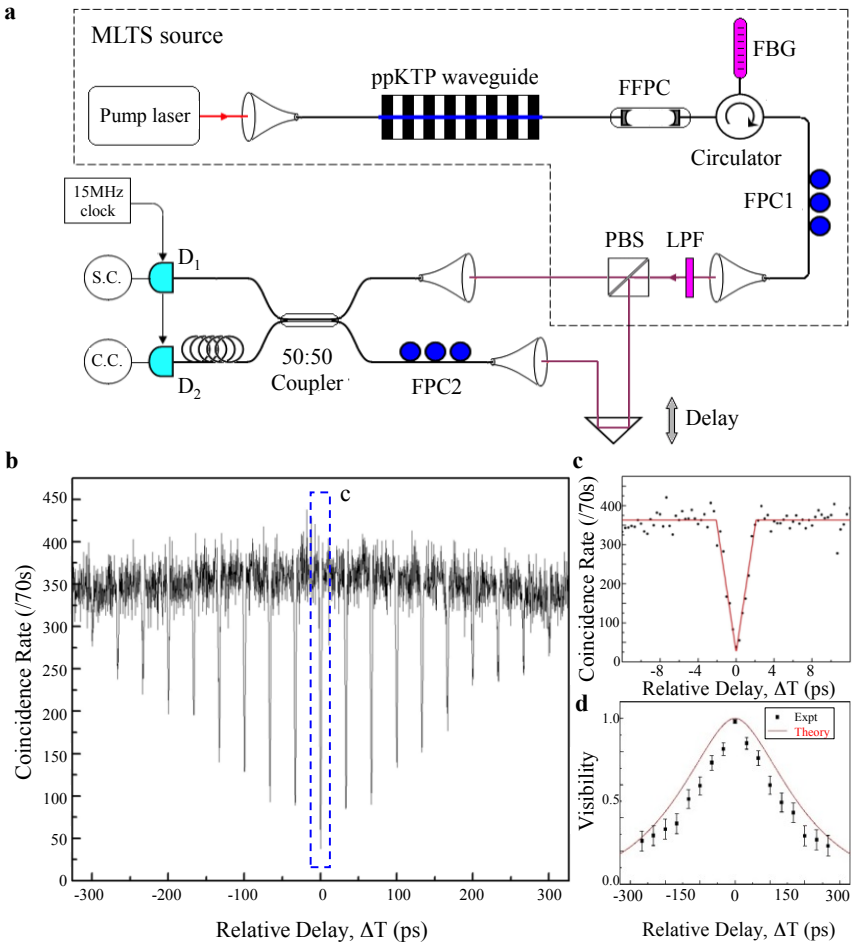

Figure 12: Generation and quantum revival observations of the high-dimensional mode-locked two-photon state. a, Illustrative experimental scheme. FFPC: fiber Fabry-Perot cavity; FBG: fiber Bragg grating; FPC: fiber polarization controller; LPF: long pass filter; PBS: polarizing beamsplitter; P: polarizer; S.C.: single counts; C.C.: coincidence counts. b, Coincidence counting rate as a function of the relative delay ΔT between the two arms of the HOM interferometer. The HOM revival is observed in the two-photon interference, with dips at 19 time-bins in this case. The visibility change across the different relative delays arises from the single frequency bin bandwidth. c, Zoom-in coincidence around zero relative delay between the two arms. The dip width was fitted to be 3.86 ± 0.30 ps, which matches well with the 245 GHz phase-matching bandwidth. The measured visibility of the dip is observed at $87.2 \pm 1.5\%$, or 96.5% after subtracting the accidental coincidence counts. d, Measured bin visibility versus HOM delay, compared with theoretical predictions.

revival of the Hong-Ou-Mandel quantum interference [39], up to 19 time-bins and with visibilities up to 96.5% as shown in Fig. 12. Moreover, frequency correlations and anti-correlations of the d-dimensional quantum state are observed as summarized in Fig. 13. We further witness the high-dimensional time-bin entanglement through a stabilized Franson interferometer. Revival of the Franson interference in the coincidence counting rate has been witnessed at the discrete time bins, where the time bin separation is the cavity round

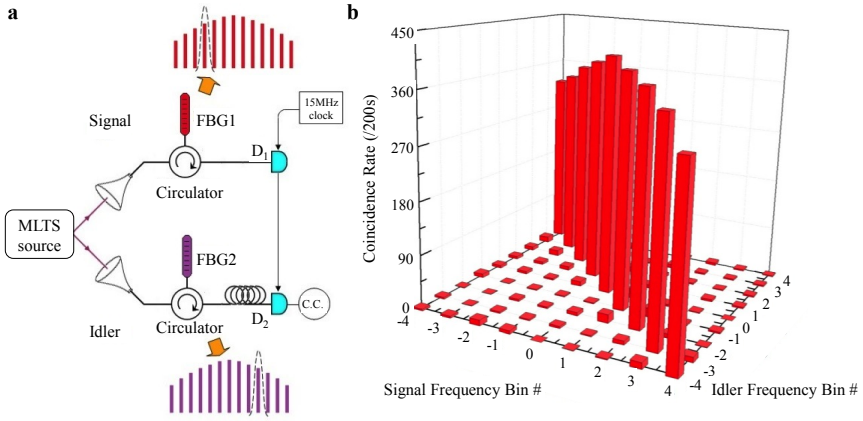

Figure 13: Quantum frequency correlation measurement of the mode-locked quantum state. a, Experimental schematic for the frequency correlation measurement. Signal and idler photons are sent to two narrow band filters for the frequency bin correlation measurement with coincidence counting. Each filter consists of a FBG and a circulator. The FBGs have matched FWHM bandwidth of 0.1 nm and are thermally tuned for the scans from -4th to +4th frequency bins from the center. b, Measured frequency correlation of the MLTS. The coincidence counting rate is recorded while the signal and idler filters are set at different frequency bin numbers.

trip time, i.e., the revival time of the mode-locked two-photon state, as shown in Fig. 14. The interference visibility is measured up to 97.8%. The bright high-dimensional frequency bin entangled state encodes 4 quantum bits per photon with high photon flux, allowing applications in dense quantum information processing and secure quantum key distribution channels.

4.4 Scalable integration of superconducting nanowire single-photon detectors on-chip

Superconducting nanowire single photon detectors (SNSPDs) are an attractive choice for integration with PICs due to their unmatched combination of sub-10-ns dead time, sub-40-ps timing jitter [40], and near-unity detection efficiency [41] in the near-infrared. The team's approach to achieving high coupling efficiencies (>50%) between superconducting nanowire single-photon detectors (SNSPDs) and incident light is the integration of these detectors with waveguides directly on the PIC. Integrating the entire optical system on a single chip reduces coupling losses and increases system scalability. However, state-of-the-art SNSPDs are fabricated using NbN films that are grown on bulk Sapphire or MgO wafers. As a result standard detectors are not suitable for integration with an existing on-chip optical system. To overcome this problem, MIT developed a process to fabricate high-performance NbN SNSPDs on membranes of silicon nitride (SiN).

Recent efforts to integrate these detectors with optical waveguides used an evanescent coupling scheme [42] in which a hairpin-shaped detector in close proximity to a waveguide absorbs the guided light via evanescent coupling. Prior work was based on the direct fabrication of SNSPDs on top of waveguides, yielding single-channel waveguide-detectors with

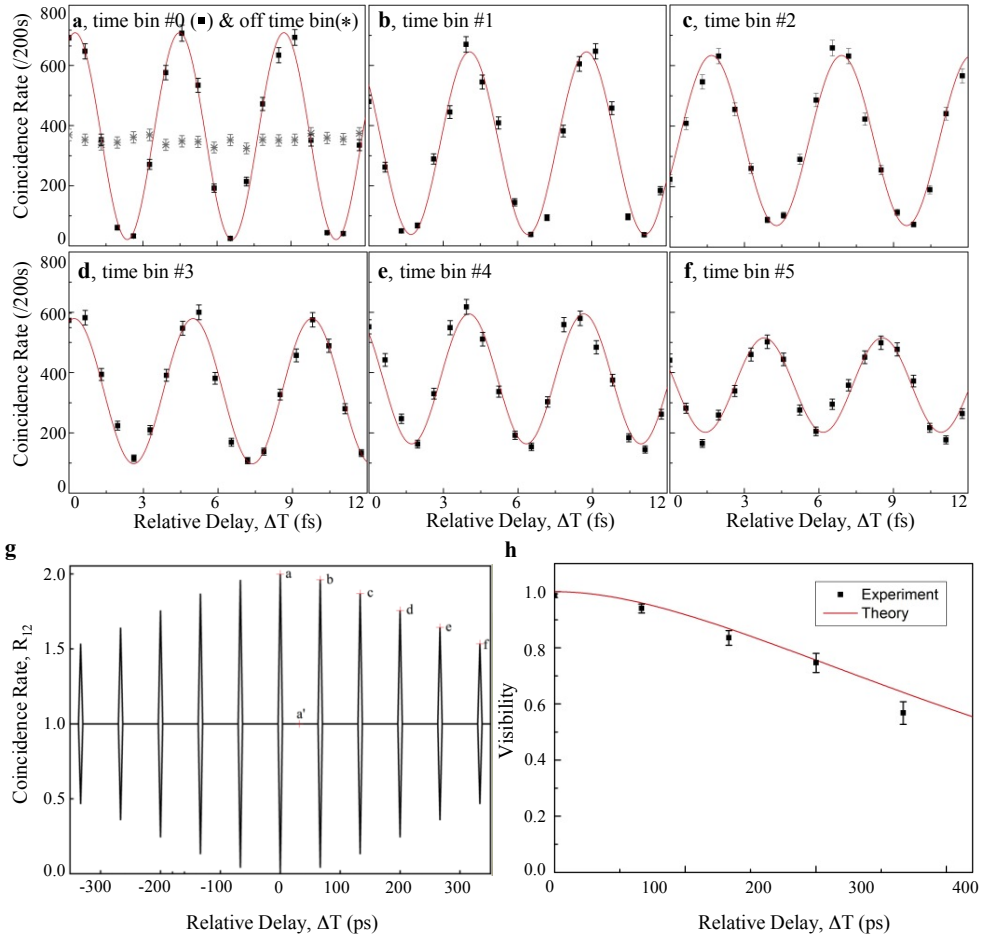

Figure 14: Measured Franson interference around different relative delays of arm2. a to f, Franson interferences at time bin #1 ($\Delta T = 0$), #2 ($\Delta T = 66.7$ ps), #3 ($\Delta T = 133.4$ ps), #4 ($\Delta T = 200.1$ ps), #5 ($\Delta T = 266.9$ ps), and #6 ($\Delta T = 333.6$ ps) respectively. Also included in the panel a is the interference measured away from the above time bins at ΔT =30 ps (stars, in panel a), with no observable interference fringes. The first datapoint in each panel (of the different relative Franson delays) includes the error bar across each data set, arising from Poisson statistics, experimental drift and measurement noise. The error bars from repeated coincidence measurements are sizably smaller than the observed coincidence rates in our measurement and setup. In each panel, the red line denotes the numerical modeling of the Franson interference on the high-dimensional quantum state. g, Theoretical fringe envelope of Franson interference for the high-dimensional mode-locked two-photon state, with superimposed experimental observations. The marked labels (a to f, and a') correspond to the actual delay points from which the above measurements are taken. h, Witnessed visibility of high-dimensional Franson interference fringes as a function of ΔT. The experimental (and theoretical) witnessed visibilities for the k-th order peaks are 97.8% (100%), 93.3% (96.0%), 83.0% (86.8%), 74.1% (75.6%), 59.0% (64.0%), and 45.4% (53.3%) respectively.

20% [43] and up to near-unity quantum efficiency [44]. However, this approach was not scalable to multiple detectors within the same photonic circuit since the yield of SNSPDs, based on sub-100-nm-wide 4-nm-thick niobium nitride (NbN) nanowires, is limited by defects at

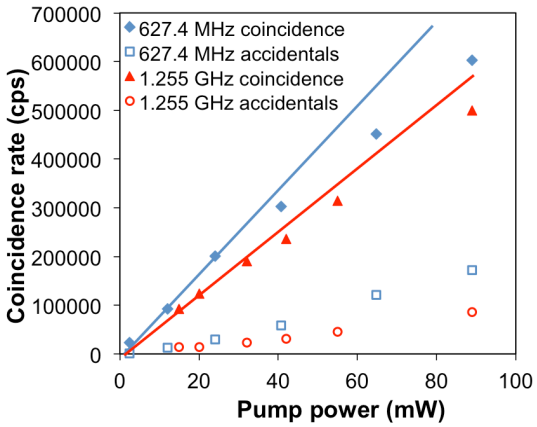

Figure 15: Maximum pair generation rate: 8.9×10^8 pairs/s at 89 mW pump. Detector donditions: 627.4 MHz (1.255 GHz) sinusoidal gating with duty cycle of 0.25, measuring 773 kcps (586 kcps) raw coincidences.

the nanoscale [45], resulting in sub-1% efficiency per detector [46] for a circuit with only two detectors. In light of these limitations scaling to larger number of high-performance detectors within the same photonic circuit is challenging.

The micro-scale flip-chip process developed in this program solves these yield problems and allows for the integration of an almost arbitrary number of high-performance detectors on high-performance PICs (limited practically only by the high-speed readout from the cryostat). Fig. 17(a) illustrates a sketch of our method in which the detectors were fabricated on thin membranes and transferred onto waveguides. Through careful pre-transfer selection of detectors large arrays of high-performance on-chip integrated detectors (Fig. 1(b)). We tested a linear optical network with two input and four output ports, each coupled to an on-chip single-photon detector. This circuit, shown in Fig. 1(c), was used to perform the first on-chip heralded measurement of the correlation function $g^{(2)}(\tau)$ of photon pairs generated from spontaneous parametric down conversion. We additionally showed that these detectors have sub-50-ps jitter and sub-10-ps dead time with high system and on-chip efficiency, making them suitable for high-speed time-encoded quantum key distribution (QKD) protocols. These measurements provide a method for integrating high-performance detectors on complex optical circuits and a step towards scalable quantum information processing on-chip.

We characterized the proof-of-concept PIC chip, shown in Fig. 17(c), with four membrane-detectors integrated with two directional couplers. Light was coupled into the silicon waveguides via lensed-fiber coupling into an inverse taper. We achieved roughly 3 dB insertion loss with this method. The resulting system detection efficiency (SDE) is shown in Fig. 19(a). The SDE includes all losses (coupling and transmission losses) between the input fiber port outside the cryostat and the detector. The detectors sub-50ps and 10-35% on-chip detection efficiency (2-8.5% system efficiency) at 800k system dark counts per second. This corresponds to a maximum system efficiency of 19% for input A and 7% system efficiency for input B, an improvement by three orders of magnitude compared to previous approaches

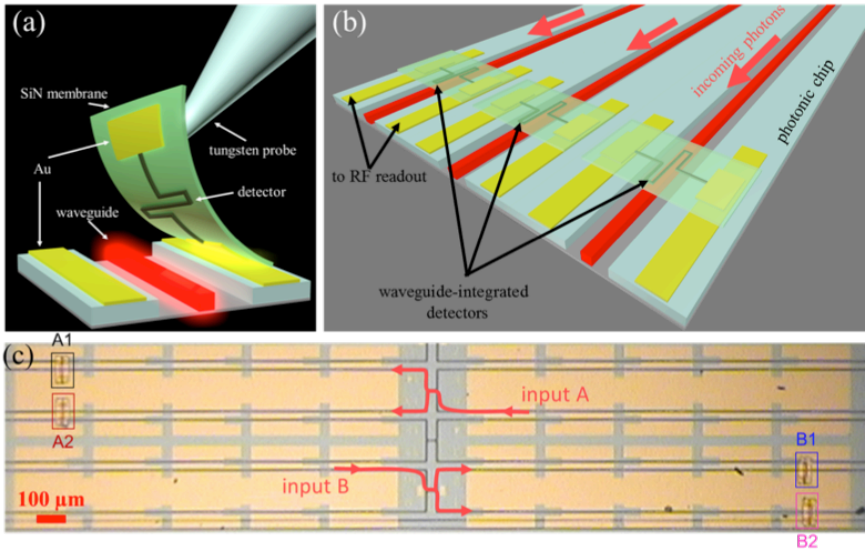

Figure 17: (a) Schematic sketch of integration of superconducting single-photon detectors with photonic waveguides via physical transfer of the detector fabricated on top of a thin carrier membrane. (b) Sketch of resulting on-chip detector array using the concept shown in (a). (c) Top-down optical micrograph of photonic chip with 4 integrated detectors.

at multi-detector integration.

5 QKD System Demonstrations

5.1 Coding

A central component of the QKD demos is to understand the fundamental limits of secure optical channels. MIT completed the information theoretic key-rate analysis for QKD schemes using an optical channel with 1) a normal transmitter, and 2) a temporally-entangled photon source; see Ref. [47]. In both cases we assume that the terminals are restricted to direct detection. In the first case, maximum key rate behaves very much like the capacity of the Poisson channel (for normal, not necessarily secret, data transmission). In particular, if Fock states can be transmitted, photon efficiency scales like minus logarithm of the average photon number per channel use; while if only coherent states can be transmitted, then we lose a double-logarithmic term. Furthermore, PPM is close to optimal for both Fock-state and coherent-state inputs. In the second case, maximum photon efficiency is approximately the same as in the first case. However, in this case, restricting to a "naive" PPM coding scheme induces the double-logarithmic loss (which is observed in the first case when coherent-state inputs are used). Most of this loss can be retrieved using a more elaborate code.

The second component of the coding analysis focused on the design of efficient codes and algorithms for establishing a secret key between two parties, named Alice and Bob, in high-dimensional QKD systems. In such systems, the observation time is typically partitioned into frames of fixed duration, with pulse-position modulation (PPM) coding used within each frame, via which a secret key is established between the parties. In Ref. [48], we derived an

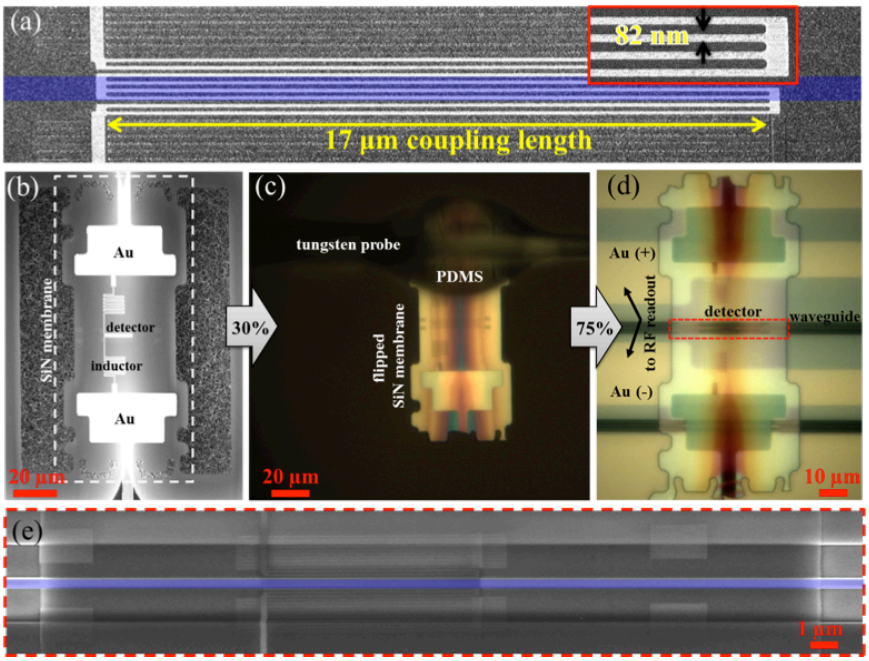

Figure 18: (a) Scanning Electron Micrograph (SEM) of a superconducting single-photon detector based on 82-nm-wide superconducting nanowires. The purple strip marks the intended location of the waveguide after the integration is complete. The meander-shaped detector is surrounded by a grid of dummy structures (parallel lines in dark grey) required to improve e-beam exposure dose uniformity resulting in higher nanowire uniformity (see SI for details on exposed pattern). The length of the detector is given by the minimum coupling length required to reach >50% optical absorption in the detector, which was obtained from optical simulations (see SI). The inset shows a locally-magnified SEM of the detector. (b) SEM of suspended SiNx membrane with detector on top. (c) The membrane-detector was removed from the carrier chip using a tungsten microprobe covered with PDMS. The membrane was then flipped and the detector aligned to the waveguide under an optical microscope. The gold pads on the membrane contacted matching gold pads on the waveguide substrate. (d) Optical micrograph of membrane-detector integrated with a silicon waveguide. (e) Top-down SEM of waveguide-integrated detector located within the region marked by a dashed line in (d) The silicon waveguide is highlighted in purple.

efficient class of schemes with adaptive frame size whose performance can converge to the fundamental limit more quickly than conventional simple PPM. With PPM schemes, Alice and Bob's observations are converted into large-alphabet sequences, but with many errors. Efficient error correction and privacy amplification are further required. We notice that well-studied Reed-Solomon codes are not efficient (or even capable) in our key-distribution applications where the symbol error rate is very high. As a result, in [49] we introduced a practical scheme called layered scheme for correcting errors in large-alphabet secret key distribution. Both theoretical analyses and simulation results show that layered schemes have near-optimal performances on q-ary channels such as uniform-error channels and limited-magnitude-error channels. In addition, in [50] we investigate privacy-amplification methods with simple and efficient hardware implementations, in particular, linear transformations based on low-

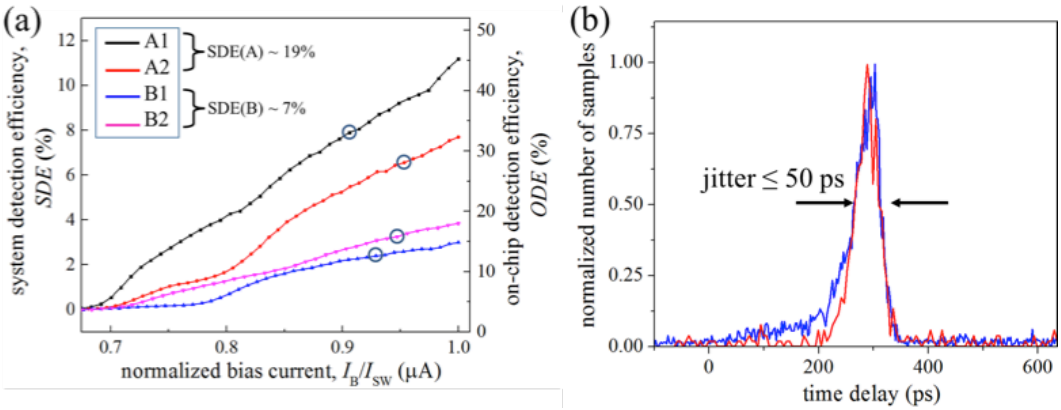

Figure 19: (a) System detection efficiency vs. normalized bias current of the waveguide-integrated detectors shown in Fig. 1(c). The bias current (IB) on the vertical axis was normalized by the maximum bias current (switching current ISW) of the detector, namely ISW(A1)=, ISW(B2), The circles mark the bias point (operation point OP) chosen for subsequent photon coincidence measurements. The OP were XXuA (A1), XXuA (A2), XXuA (A3) and XX uA (A4). (b) Instrument Response Function of the waveguide-detectors shown in Fig. 1(c). The detectors were biased at the operation points marked in (a).

density random matrices. We show that this method can achieve the information-theoretical upper bound on efficiency for a wide range of key-distribution systems. By combining all the techniques above developed for modulation, error correction and privacy amplification, we can achieve a practical protocol for high-dimensional QKD with performance close to the information-theoretical limit.

The experimental demonstrations focused on several implementations, as will be discussed now.

5.2 DO-QKD Implementation

The major components of the DO-QKD demo are sketched in Fig. 20. Entangled photon pairs are produced by an SPDC source held by Alice. Alice keeps one photon in each pair and sends the other to Bob. Alice and Bob detect their photons in two conjugate measurement bases — either directly or after normal/anomalous group velocity dispersion. The shared timing correlations between pairs of detected photons are used to produce the key. The detectors are WSi SNSPDs [41] provided by the group of Sae Woo Nam of NIST. The group velocity dispersion comes from dispersion compensation modules produced by TeraXion, providing ≈ 600 ps/nm of normal/anomalous dispersion.

To bound an eavesdropper's information about the key, Alice and Bob must measure the increase in the frequency correlations between their photons. We assume that direct detection measurements are used to generate key and measurements made using group velocity dispersion are used as a security check; therefore, by quantifying the increase in the frequency correlations, Alice and Bob can learn an eavesdropper's effects on their direct detection measurements. The baseline frequency correlation is determined by σ_{coh}, the coherence time of the SPDC pump field. The observable increase in the correlation, and therefore, the upper

bound on the eavedropper's information, is limited by hardware — both the detectors and the dispersive elements. In the current system, an eavesdropper can obtain a maximum of 1.09 bpc, or bits per detected photon coincidence. Preliminary tests suggest the possibility of obtaining at least 4 secure bits per coincidence. Details are described in a manuscript to be submitted [51].

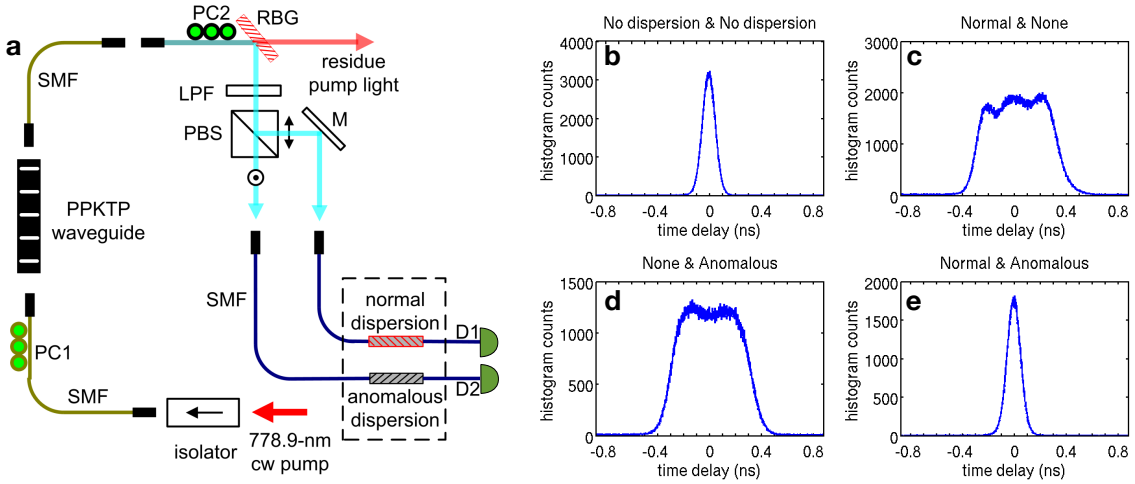

Figure 20: (a) Experimental setup for DO-QKD experiment, using degenerate entangled photon pairs created with by SPDC in a PPKTP waveguide and detected either directly or after normal/anomalous group velocity dispersion. (b-e) Coincidence measurements across detectors D1 and D2 for the four combinations of direct detection and normal/anomalous dispersion. Clearly, the variance is small when both Alice and Bob measure directly or after normal/anomalous dispersion; in the other cases, the uncertainty is greatly increased to $\approx$ 600ps, the GVD delay of the dispersive optics systems, as expected.

5.3 Implementations of high-dimensional QKD

Led by Tian Zhong and co-PI Franco Wong we demonstrated the full high-dimensional QKD (HDQKD) protocol whose security against collective Gaussian attacks was achieved through high-visibility Franson interferometry. Two experimental implementations of the full protocol were realized. The first implementation was based on time-energy entangled photons generated from the PPKTP waveguide source via SPDC, and we used self-differencing InGaAs APDs as single-photon detectors that were gated on at a frequency of 1.26 GHz. The experimental setup for entanglement-based HDQKD is shown in Fig. 21. The orthogonally polarized entangled photons were coupled into a single-mode fiber and separated by a polarizing beam splitter. The photons at Alice and Bob were passively switched using 50:50 fiber beam splitters between key generation and Franson interferometry. Figure 22 shows the optimized results for the secure key rates without and with 5 dB of extra loss that simulates a 25-km fiber link. For a frame size of 64 bins, each with bin duration of 793 ps (inverse of gating frequency), and a photon-pair generation rate of 0.31% per bin, we achieved 4 secure bits per photon-pair coincidence and a secure bit rate of 89 kb/s. The

measured results include passing the raw data through error correction and estimating the secure key rate after privacy amplification. The additional 5 dB loss reduces the secure rate, as expected, but does not affect the secure bit per photon-pair efficiency. Security in both cases was provided by the measured Franson visibility of 99.6% relative to the theoretically achievable visibility of 99.8% that was limited by the pump's MHz bandwidth. Compared with binary encoding such as the state-of-the-art BBM92 implementation based on polarization entangled photons [A. Treiber *et al.* New J. Phys. **11,** 045013 (2009)] with a 12.5 kb/s rate, our results demonstrate a clear improvement in photon information efficiency ($> 10\times$) and QKD throughput ($7\times$).

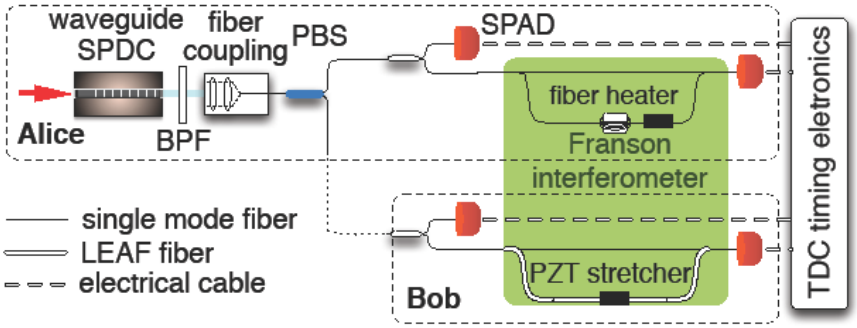

Figure 21: Experimental Setup for HDQKD implementation using time-energy entangled photons. BPF: band-pass filter, PBS: polarizing beam splitter, TDC: time-to-digital converter.

Extra loss	photon/bin	frame size	QSER	secure bpp	ECC	secure key rate
none	0.0031	64	14 %	4.05	layered LDPC	89 kbps
5 dB	0.0031	64	14 %	4.05	layered LDPC	28 kbps

Figure 22: Operating parameters and results for entanglement-based HDQKD implementation.

Our second implementation used an attenuated broadband noise source in a pulse-position modulation scheme in conjunction with entanglement-based Franson security checks, as shown in Fig. 23. The classical broadband noise source was derived from the amplified spontaneous emission (ASE) of an erbium-doped fiber amplifier (EDFA) output and a high-speed fiber intensity modulator randomly chose a time bin for PPM transmission. Using an optical switch Alice randomly chose to send either the ASE light (70%) or the SPDC entanglement source output (30%) to Bob. A spectral filter ensured that the light received by Bob was spectrally indistinguishable. Bob used a 50-50 fiber beam splitter to passively choose either key generation or Franson interferometry. We obtained a Franson visibility similar to that obtained in the entanglement-based HDQKD implementation. Figure 24 shows the operating conditions and the optimized results for the PPM implementation that yields 2.9 secure bits per detected photon and a 7.3 Mb/s secure key rate, suggesting that HDQKD with the classical PPM implementation can significantly improve the overall secure key rate. We should point out that the entanglement-based HDQKD protocol is currently

limited by the low efficiency (18%) of the InGaAs detectors and the ~25% duty cycle in the gating operation of the detectors. We expect a 50- to 100-fold secure key rate improvement if efficient superconducting nanowire detectors such as WSi detectors are used.

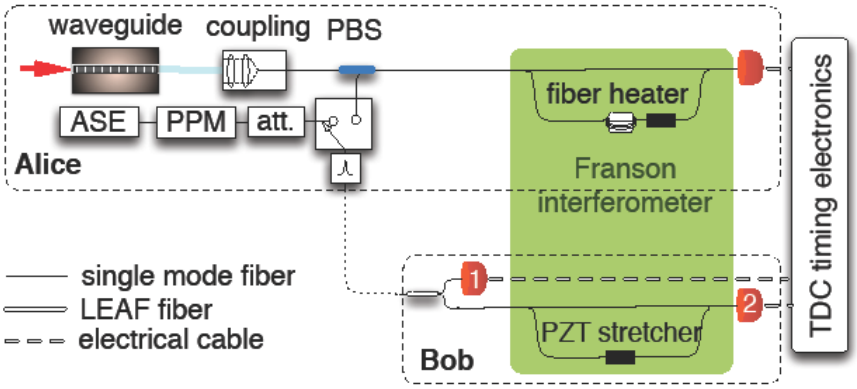

Figure 23: Experimental Setup for HDQKD implementation using an ASE source and PPM. A fast intensity modulator with a pseudo-random bit sequence input places the ASE light into the chosen time bin within the PPM frame. A second pseudo-random bit sequence input to a fast optical switch transmits the PPM frame containing ASE photons or the Franson frame containing the SPDC photons in a 70:30 ratio. PBS: polarizing beam splitter, TDC: time-to-digital converter.

photon/frame	frame size	QSER	secure bpp	ECC	secure key rate
1.3	16	9.5 %	2.9	layered LDPC	7.3 Mbps

Figure 24: Operating parameters and optimized results for HDQKD implementation using an ASE source and PPM.

6 Publications and Presentations

In addition to four manuscripts currently being finished for publication, the following journal articles were published:

6.1 Journal Publications

1. Directional free-space coupling from photonic crystal waveguides, C.-C. Tsai, J. Mower, and D. Englund, Opt. Express 19 (21), 20586-96 (2011)

2. Efficient generation of single and entangled photons on a silicon photonic integrated chip, J. Mower and D. Englund, Phys. Rev. A 84 (2011)

3. Zero phase delay in negative-index photonic crystal superlattices, S. Kocaman, M.S. Aras, P. Hsieh, J. F. McMillan, C. G. Biris, N. C. Panoiu, M. B. Yu, D. L. Kwong, A. Stein, and C. W. Wong, Nature Photonics 5, 499 (2011).

4. Private-Capacity Bounds for Bosonic Wiretap Channels, L. Wang, J. H. Shapiro, N.Chandrasekaran, and G. W. Wornell, ArXiv:1202.1126 (2012) "Efficient single-spatial-mode periodically poled KTiOPO4 waveguide source for high- dimensional entanglement-based quantum key distribution," Tian Zhong, Franco N. C. Wong,

5. Alessandro Restelli, and Joshua C. Bienfang, Opt. Express, 20, Issue 24, pp. 26868-26877 (2012)

6. Xuetao Gan, Kin Fai Mak, Yuanda Gao, Yumeng You, Fariba Hatami, James Hone, Tony F. Heinz, and Dirk Englund. Strong enhancement of light-matter interaction in graphene coupled to a photonic crystal nanocavity. Nano Letters, 12(11):5626-5631, 2012.

7. High-dimensional quantum key distribution using dispersive optics, J. Mower, P. Desjardins, J. H. Shapiro, D. Englund, Phys. Rev. A 87 (2013).

8. N. Chandrasekaran and J. H. Shapiro, "Photon information efficient communication through atmospheric turbulence – Part I: Channel model and propagation statistics," submitted to J. Lightw. Technol. (2013)

9. N. Chandrasekaran, J. H. Shapiro, and L. Wang, "Photon information efficient communication through atmospheric turbulence – Part II: Bounds on ergodic classical and private capacities," submitted to J. Lightw. Technol. (2013)

10. Xuetao Gan, Hannah Clevenson, Pierre Desjardins, Luozhou Li, and Dirk Englund. Nanophotonic filters and integrated networks in flexible 2D polymer photonic crystals. Nature Scientific Reports 3 (2145) (2013)

11. Chip-integrated ultrafast graphene photodetector with high responsivity, X. Gan, R.J. Shiue, Y. Gao, I. Meric, T. F. Heinz, K. Shepard, J. Hone, S. Assefa, & D. Englund, Nature Photonics AOP (2013)

12. X. Xu, Z. Xie, J. Zheng, J. Liang, T. Zhong, M. Yu, S. Kocaman, G.-Q. Lo, D.-L. Kwong, D. R. Englund, F. N. C. Wong, and C. W. Wong, Near-infrared Hong-Ou-Mandel interference on a silicon quantum photonic circuit, Optics Express Vol. 21(4), 5014 (2013).

13. Tian Zhong and Franco N. C. Wong. Nonlocal cancellation of dispersion in Franson interferometry. Phys. Rev. A 88, 020103(R) (2013) H. Zhou, V. Chandar, and G. Wornell. Low-density random matrices for secret key extraction. IEEE Int. Symp. Inform. Theory (ISIT) (2013)

14. Hongchao Zhou, Ligong Wang, and Gregory W. Wornell. Layered schemes for large-alphabet secret key distribution. In ITA, pages 1-10 (2013)

15. Hongchao Zhou and Gregory Wornell. Adaptive pulse-position modulation for high-dimensional quantum key distribution. In Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on, pages 359-363 (2013)

16. Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, "Unconditional Security of Time-energy Entanglement Quantum Key Distribution using Dual-basis Interferometry", arXiv:1311.0825

17. Catherine Lee, Jacob Mower, Zheshen Zhang, Jeffrey H. Shapiro, and Dirk Englund, "Finite-key analysis of high-dimensional dispersive optics quantum key distribution," arXiv:1311.1233

6.2 Filed Patents

- Dirk Englund and Xuetao Gan, WO/2013/148349 - GRAPHENE PHOTONICS FOR RESONATOR-ENHANCED ELECTRO-OPTIC DEVICES AND ALL-OPTICAL INTERACTIONS

- Jacob Mower and Dirk Englund, WO/2013/112351 - SYSTEMS AND METHODS FOR TELECOMMUNICATION USING HIGH-DIMENSIONAL TEMPORAL QUANTUM KEY DISTRIBUTION

- Jacob Mower and Dirk Englund, WO/2013/009946 - CHIP INTEGRATED SINGLE PHOTON GENERATION BY ACTIVE TIME MULTIPLEXING

- Jacob Mower and Dirk Englund, WO/2013/103431 - SYSTEMS AND METHODS FOR COUPLING ELECTROMAGNETIC RADIATION FROM FIBER ARRAYS INTO WAVEGUIDES AND PHOTONIC CHIPS

- WONG, Chee, Wei; (US)., WONG, Franco, N.c.; (US)., ENGLUND, Dirk, R.; (US), WO/2013/052903 - CHIP-SCALE INTERFEROMETRY FOR HYPERENTANGLEMENT PROCESSING

- ENGLUND, Dirk; (US)., MOWER, Jacob; (US)., NAJAFI, Faraz; (US)., HU, Xiaolong; (US), BERGGREN, Karl, K.; (US), WO2013112208) - COMPACTLY-INTEGRATED OPTICAL DETECTORS AND ASSOCIATED SYSTEMS AND METHODS

- ENGLUND, Dirk; SYSTEMS AND METHODS FOR MULTILEVEL OPTICAL STORAGE IN TUNABLE PHOTONIC CRYSTAL CAVITIES

6.3 Conference Papers

- T. Zhong, F. N. C. Wong, A. Restelli, and J. C. Biefang, "Efficient single-spatial-mode PPKTP waveguide source for high dimensional entanglement-based QKD," to be presented at CLEO/QELS 2012, paper JTh1K3.

- T. Zhong and F. N. C. Wong, "Franson interferometry with 99.6% visibility via fiberoptic dispersion engineering," in 11th International Conference on Quantum Communication, Measurement and Computing, Vienna, Austria, July 2012, paper accepted for presentation.

- D. Englund and J. Mower, "Quantum Optics on Silicon Photonic Chips", Invited Paper at Frontiers In Optics (San Jose, CA, Oct. 18, 2011)
- On High-Efficiency Optical Communication and Key Distribution, Yuval Kochman and Gregory W. Wornell, ITA, San Diego (2012)
- Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, submitted to IEEE International Symposium on Information Theory (2012)
- F. N. C. Wong, "Time-energy entangled waveguide source for high-dimensional QKD," in Laser Science XXVII, San Jose, CA, October 2011, invited paper LTuF$_4$.
- J. Mower and D. Englund, "High-dimensional quantum key distribution using dispersive optics," submitted for Frontiers in Optics, Rochester, NY, 2012
- Ligong Wang Yuval Kochman and Gregory W. Wornell. Toward photon-efficient key distribution over optical channels. Submitted to IEEE Transactions on Information Theory, 2013.
- H. Zhou and G. Wornell. Adaptive pulse-position modulation for high-dimensional quantum key distribution.
- Hongchao Zhou, Ligong Wang, and Gregory W. Wornell. Layered schemes for large-alphabet secret key distribution. In ITA, pages 1-10, 2013.
- H. Zhou, V. Chandar, and G. Wornell. Low-density random matrices for secret key extraction. IEEE Int. Symp. Inform. Theory (ISIT), 2013.

References

[1] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[2] Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, and Dirk Englund. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A*, 87:062322, Jun 2013.

[3] Zheshen Zhang, Jacob Mower, Dirk Englund, Franco N. C. Wong, and Jeffrey H. Shapiro. Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry. *arXiv:1311.0825*, 2013.

[4] Nivedita Chandrasekaran and Jeffrey H. Shapiro. Photon information efficient communication through atmospheric turbulence — part i: Channel model and propagation statistics. *under review*, 2013.

[5] Nivedita Chandrasekaran, Jeffrey H. Shapiro, and Ligong Wang. Photon information efficient communication through atmospheric turbulence — part ii: Bounds on ergodic classical and private capacities. *under review*, 2013.

[6] Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell. Private-capacity bounds for bosonic wiretap channels. 2012.

[7] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.

[8] C. H. Bennett and G. Brassard. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[9] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[10] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of Quantum Key Distribution Using d-Level Systems. *Phys. Rev. Lett.*, 88(12):127902, Mar 2002.

[11] Lijian Zhang, Christine Silberhorn, and Ian A. Walmsley. Secure Quantum Key Distribution using Continuous Variables of Single Photons. *Phys. Rev. Lett.*, 100:110504, Mar 2008.

[12] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum Cryptography Using Entangled Photons in Energy-Time Bell States. *Phys. Rev. Lett.*, 84:4737–4740, May 2000.

[13] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin. Bell-Type Test of Energy-Time Entangled Qutrits. *Phys. Rev. Lett.*, 93:010503, Jul 2004.

[14] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States. *Phys. Rev. Lett.*, 98:060503, Feb 2007.

[15] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin. Experimental investigation of the robustness of partially entangled qubits over 11 km. *Phys. Rev. A*, 66:062304, Dec 2002.

[16] B. Qi. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Optics letters*, 31(18):2795–2797, 2006.

[17] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.

[18] Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication. *Phys. Rev. Lett.*, 89:240401, Nov 2002.

[19] G. Molina-Terriza, A. Vaziri, J. Řeháček, Z. Hradil, and A. Zeilinger. Triggered Qutrits for Quantum Communication Protocols. *Phys. Rev. Lett.*, 92:167903, Apr 2004.

[20] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States. *Phys. Rev. Lett.*, 98(6):060503, Feb 2007.

[21] Lijian Zhang, Christine Silberhorn, and Ian A. Walmsley. Secure quantum key distribution using continuous variables of single photons. *Phys. Rev. Lett.*, 100:110504, Mar 2008.

[22] J. Nunn, L. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *ArXiv*, 2013.

[23] Miguel Navascués and Antonio Acín. Security Bounds for Continuous Variables Quantum Key Distribution. *Phys. Rev. Lett.*, 94:020505, Jan 2005.

[24] Raúl García-Patrón and Nicolas J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[25] Jacob Mower, Zheshen Zhang, Pierre Desjardins, Catherine Lee, Jeffrey H. Shapiro, and Dirk Englund. High-dimensional quantum key distribution using dispersive optics. *Phys. Rev. A*, 87:062322, Jun 2013.

[26] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.*, 77:2818–2821, Sep 1996.

[27] J. D. Franson. Nonlocal cancellation of dispersion. *Phys. Rev. A*, 45:3126–3132, Mar 1992.

[28] Thomas Brougham, Stephen M Barnett, Kevin T McCusker, Paul G Kwiat, and Daniel J Gauthier. Security of high-dimensional quantum key distribution protocols using franson interferometers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 46(10):104010, 2013.

[29] Tian Zhong and Franco N. C. Wong. Nonlocal cancellation of dispersion in franson interferometry. *Phys. Rev. A*, 88:020103, Aug 2013.

[30] J. D. Franson. Two-photon interferometry over large distances. *Phys. Rev. A*, 44:4552–4555, Oct 1991.

[31] Yurii Vlasov, William M. J. Green, and Fengnian Xia. High-throughput silicon nanophotonic wavelength-insensitive switch for on-chip optical networks. *Nat. Photon*, 2:242–246, 2008.

[32] Xuetao Gan, Ren-Jye Shiue, Yuanda Gao, Inanc Meric, Tony F. Heinz, Kenneth Shepard, James Hone, Solomon Assefa, and Dirk Englund. Chip-integrated ultrafast graphene photodetector with high responsivity. *Nature Photonics*, 2013.

[33] Scalable single-photon detection on a photonic chip. F. najafi and j. mower and n. harris and f. bellei and a. dane and c. lee and x. hu and p. kharel and f. marsili and s. assefa and k. k. berggren and d. englund. *to be submitted*, 2013.

[34] Xinan Xu, Zhenda Xie, Jiangjun Zheng, Junlin Liang, Tian Zhong, Mingbin Yu, Serdar Kocaman, Guo-Qiang Lo, Dim-Lee Kwong, Dirk R. Englund, Franco N. C. Wong, and Chee Wei Wong. Near-infrared hong-ou-mandel interference on a silicon quantum photonic chip. *Opt. Express*, 21(4):5014–5024, Feb 2013.

[35] KocamanS., ArasM. S., HsiehP., McMillanJ. F., BirisC. G., PanoiuN. C., YuM. B., KwongD. L., SteinA., and WongC. W. Zero phase delay in negative-refractive-index photonic crystal superlattices. *Nat Photon*, 5(8):499–505, 08 2011.

[36] Tian Zhong, Franco N. C. Wong, Alessandro Restelli, and Joshua C. Bienfang. Efficient single-spatial-mode periodically-poled ktiopo4 waveguide source for high-dimensional entanglement-based quantum key distribution. *Opt. Express*, 20(24):26868–26877, Nov 2012.

[37] Paul G. Kwiat, Edo Waks, Andrew G. White, Ian Appelbaum, and Philippe H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:R773–R776, Aug 1999.

[38] F.N.C. Wong, J.H. Shapiro, and T. Kim. Efficient generation of polarization-entangled photons in a nonlinear crystal. *Laser Physics*, 16(11):1517–1524, 2006.

[39] Z. Xie, T. Zhong, X. Xu, J. Liang, Y.-X. Gong, J. H. Shapiro, F. N. C. Wong, and C. W. Wong. High-dimensional frequency entanglement of mode-locked two-photon states. *submitted*, 2013.

[40] F. Najafi, F. Marsili, E. Dauler, R.J. Molnar, and K.K. Berggren. Timing performance of 30-nm-wide superconducting nanowire avalanche photodetectors. *Applied Physics Letters*, 100(15):152602–152602–4, 2012.

[41] MarsiliF., VermaV. B., SternJ. A., HarringtonS., LitaA. E., GerritsT., VayshenkerI., BaekB., ShawM. D., MirinR. P., and NamS. W. Detecting single infrared photons with 93% system efficiency. *Nat Photon*, 7(3):210–214, 03 2013.

[42] Xiaolong Hu, C.W. Holzwarth, D. Masciarelli, E.A. Dauler, and K.K. Berggren. Efficiently Coupling Light to Superconducting Nanowire Single-Photon Detectors. *Applied Superconductivity, IEEE Transactions on*, 19(3):336–340, june 2009.

[43] J. P. Sprengers, A. Gaggero, D. Sahin, S. Jahanmirinejad, G. Frucci, F. Mattioli, R. Leoni, J. Beetz, M. Lermer, M. Kamp, S. Höfling, R. Sanjines, and A. Fiore. Waveguide superconducting single-photon detectors for integrated quantum photonic circuits. *Applied Physics Letters*, 99(18):–, 2011.

[44] Carsten Schuck, Wolfram H. P. Pernice, and Hong X. Tang. Waveguide integrated low noise nbtin nanowire single-photon detectors with milli-hz dark count rate. *Sci. Rep.*, 3, 05 2013.

[45] Andrew J. Kerman, Eric A. Dauler, Joel K. W. Yang, Kristine M. Rosfjord, Vikas Anant, Karl K. Berggren, Gregory N. Gol'tsman, and Boris M. Voronov. Constriction-limited detection efficiency of superconducting nanowire single-photon detectors. *Applied Physics Letters*, 90(10):–, 2007.

[46] Döndü Sahin, Alessandro Gaggero, Thang Ba Hoang, Giulia Frucci, Francesco Mattioli, Roberto Leoni, Johannes Beetz, Matthias Lermer, Martin Kamp, Sven Höfling, and Andrea Fiore. Integrated autocorrelator based on superconducting nanowires. *Opt. Express*, 21(9):11162–11170, May 2013.

[47] Ligong Wang Yuval Kochman and Gregory W. Wornell. Toward photon-efficient key distribution over optical channels. *Submitted to IEEE Transactions on Information Theory*, 2013.

[48] Hongchao Zhou and Gregory Wornell. Adaptive pulse-position modulation for high-dimensional quantum key distribution. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 359–363, 2013.

[49] Hongchao Zhou, Ligong Wang, and Gregory W. Wornell. Layered schemes for large-alphabet secret key distribution. In *ITA*, pages 1–10, 2013.

[50] H. Zhou, V. Chandar, and G. Wornell. Low-density random matrices for secret key extraction. *IEEE Int. Symp. Inform. Theory (ISIT)*, 2013.

[51] Catherine Lee, Zheshen Zhang, Jacob Mower, Franco N. C. Wong, Jeffrey H. Shapiro, and Dirk Englund. Experimental demonstration of high-dimensional quantum key distribution using dispersive optics. *to be submitted*, 2013.